



SEALED

In Re: Sealed Warrants
(Case No. 2:17-cv-02775-JAD-PAL)

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard South,
Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336



FILED

2017 OCT 13 PM 12:30

U.S. MAGISTRATE JUDGE

BY _____

SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

FILED

2017 OCT 13 PM 12:30

U.S. MAGISTRATE JUDGE

BY _____

STEVEN W. MYHRE
Acting United States Attorney
District of Nevada
CRISTINA D. SILVA
PATRICK BURNS
Assistant United States Attorneys
501 Las Vegas Blvd. South, Ste. 1100
Las Vegas, Nevada 89101
Telephone: (702) 388-6336
Fax (702) 388-6698
john.p.burns@usdoj.gov

Attorney for the United States of America

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

-oOo-

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
EMAIL ACCOUNT
CENTRALPARK1@LIVE.COM THAT IS
STORED AT A PREMISES
CONTROLLED BY MICROSOFT.

A1

Magistrate No. 2:17-mj-01009-NJK

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH
WARRANTS

(Under Seal)

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
EMAIL ACCOUNT
MARILOUROSES@LIVE.COM THAT IS
STORED AT A PREMISES
CONTROLLED BY MICROSOFT.

A2

Magistrate No.

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH
WARRANTS

(Under Seal)

STATE OF NEVADA)
) ss:
COUNTY OF CLARK)

///

///

1
2 **AFFIDAVIT IN SUPPORT OF AN**
 APPLICATION FOR SEARCH WARRANTS

3 I, Zachary C. McKinney, Special Agent, Federal Bureau of Investigation (FBI),
4 having been duly sworn, hereby depose and say:

5 **INTRODUCTION AND AGENT BACKGROUND**

6 1. Your Affiant makes this affidavit in support of an application for search
7 warrants for information associated with email accounts centralpark1@live.com ("Target
8 Account 1") and marilouroses@live.com ("Target Account 2"). Target Account 1 is an
9 account associated with STEPHEN PADDOCK. Target Account 2 is an account
10 associated with MARILOU DANLEY. The information associated with both accounts is
11 stored at a premises owned, maintained, controlled, or operated by Microsoft
12 Corporation ("Microsoft"), an American multinational technology company based in
13 Redmond, Washington that specializes in Internet-related services and products along
14 with the development and manufacturing of computer-related items. Those online
15 services include, but are not limited to, email services, cloud computing, and many other
16 services. The information to be searched is described in the following paragraphs and in
17 Attachment "A" (attached hereto and incorporated herein by reference). This affidavit is
18 made in support of an application for search warrants under 18 U.S.C. §§ 2703(a),
19 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft to disclose to the government
20 records and other information in its possession, pertaining to the subscriber or customer
21 associated with the Target Accounts.

22 2. I am a Special Agent with the Federal Bureau of Investigation, currently
23 assigned to Las Vegas, Nevada. I have been employed as a Special Agent of the FBI since
24

1 March of 2017. Over the course of my employment with the FBI, I have conducted
2 surveillance, analyzed telephone records, interviewed witnesses, supervised activities of
3 sources, executed search warrants, and executed arrest warrants. These investigative
4 activities have been conducted in conjunction with a variety of investigations, to include
5 those involving robbery, drug trafficking, human trafficking, criminal enterprises, and
6 more. In addition to my practical experiences, I received five months of extensive law
7 enforcement training at the FBI Academy. Previous to the FBI, I was employed as a
8 human intelligence gatherer with the United States Army. I was trained extensively in
9 interrogation, interview, and source handling techniques and best practices. I also
10 received an MBA in International Business and worked with ExxonMobil as a financial
11 manager.

12 3. I make this affidavit in support of an application for a search warrant for
13 information associated with the Microsoft accounts associated with
14 centralpark1@live.com" and "marilouroses@live.com," which is stored at a premises
15 owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at
16 One Microsoft Way, Redmond, WA 98052-6399, hereinafter referred to as "premises,"
17 and further described in Attachments A-1 and A-2 hereto.

- 18 a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C.A. § 32(a);
19 b. Violence at International Airport - 18 U.S.C. § 37(a)(2); and
20 c. Unlawful Interstate Transport/Delivery of Firearms by Non Federal
21 Firearms Licensee - 18 U.S.C. §§ 922(a)(3) and (5);
22 d. Aiding and Abetting - 18 U.S.C. § 2.

1 (hereafter, "Subject Offenses") have been committed by STEPHEN PADDOCK,
2 MARILOU DANLEY, and others yet unknown. There is also probable cause to search
3 the information described in Attachment "A" for evidence of these crimes and
4 information which might reveal the identities of others involved in these crimes, as
5 described in Attachment "B" (attached hereto and incorporated herein by reference).

6 PROBABLE CAUSE

7 4. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music
8 festival, was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At
9 approximately 10:08 p.m., the Las Vegas Metropolitan Police Department (LVMPD)
10 received calls reporting shots had been fired at the concert and multiple victims were
11 struck. LVMPD determined the shots were coming from Rooms 134 and 135 on the 32nd
12 floor of the Mandalay Bay Resort and Casino, located due west of the festival rounds at
13 3950 South Las Vegas Boulevard, Las Vegas, Nevada. These rooms are an elevated
14 position which overlooks the concert venue. Witness statements and video
15 footage captured during the attack indicates that the weapons being used were firing in
16 a fully-automatic fashion.

17 5. LVMPD officers ultimately made entry into the room and located an
18 individual later identified as Stephen Paddock. Paddock was deceased from an apparent
19 self-inflicted gunshot wound.

20 6. Paddock's Nevada driver's license was located in the Mandalay Bay hotel
21 room with Paddock, and both hotel rooms were registered in his name. A player's club
22 card in name of Marilou Danley was located in Paddock's room, and the card returned
23 to the address located on Babbling Brook Street in Mesquite, Nevada. FBI Agents
24

1 located Danley, who was traveling outside the United States at the time of the
2 shooting. It was ultimately determined that Danley resided with Paddock at the
3 Babbling Brook address.

4 7. On October 2, 2017, search warrants were executed on Paddock's Mandalay
5 Bay hotel rooms, Paddock's vehicle at Mandalay Bay, and two Nevada residences owed
6 by Paddock: 1372 Babbling Brook Court in Mesquite, and 1735 Del Webb Parkway in
7 Reno, Nevada. Officers and Agents found over 20 firearms, hundreds of rounds of
8 ammunition, and hundreds of spent shell casings in the Mandalay Bay hotel rooms, in
9 close proximity to Paddock's body. Over a thousand rounds of rifle ammunition and 100
10 pounds of explosive material was found in Paddock's vehicle. Additional explosive
11 material, approximately 18 firearms, and over 1,000 rounds of ammunition was located
12 at the Mesquite residence. A large quantity of ammunition and multiple firearms were
13 recovered from the Reno residence.

14 8. As of this date, 58 people have been identified to have been killed in
15 Paddock's attack and another 557 were reportedly injured. Additionally, investigators
16 discovered that STEPHEN PADDOCK also utilized a firearm to shoot large fuel tanks
17 on Las Vegas McCarran International Airport property. Multiple bullet holes were found
18 on the tank, which investigators believe was an attempt by STEPHEN PADDOCK to
19 cause the tanks to explode.

20 9. In an effort to determine whether or not STEPHEN PADDOCK was
21 assisted and/or conspired with unknown individuals, investigators have attempted to
22 identify all of STEPHEN PADDOCK's associated. It was quickly determined that a
23 casino player's card in the name of MARILOU DANLEY was located in the room at the
24

1 time of the attack. She has been identified thus far as the most likely person who aided
2 or abetted STEPHEN PADDOCK based on her informing law enforcement that her
3 fingerprints would likely be found on the ammunition used during the attack.
4 Subsequently, investigators worked to identify the communication facilities utilized by
5 STEPHEN PADDOCK and MARILOU DANLEY.

6 10. Based on a review of STEPHEN PADDOCK's financial accounts, Target
7 Account 1 was determined to belong to STEPHEN PADDOCK. On October 3, 2017,
8 investigators requested an emergency disclosure of records from Microsoft related to
9 Target Account 1 so it could be immediately searched for any evidence of additional co-
10 conspirators. Unfortunately, the information was only requested for a six-month
11 timeframe. Within the account, investigators identified Target Account 2 as one that
12 belonged to MARILOU DANLEY, which was clear based on the communications
13 between the two email accounts. In an interview, DANLEY stated that PADDOCK had
14 access to one of her email accounts, which investigators believe to be Target Account 2.

15 11. On September 25, 2017, an email was exchanged between the Target
16 Accounts which discussed a wire transfer of funds which was to be sent by STEPHEN
17 PADDOCK to MARILOU DANLEY. It is unclear what the purpose of the wire transfer
18 was, but MARILOU DANLEY is known to have been in the Philippines at the time.

19 12. Additionally, on July 6, 2017, Target Account 1 sent an email to
20 centralpark4804@gmail.com which read, "try an ar before u buy. we have huge selection.
21 located in the las vegas area." Later that day, an email was received back from
22 centralpark4804@gmail.com to Target Account 1 that read, "we have a wide variety of
23 optics and ammunition to try." And lastly, Target Account 1 later sent an email to
24

1 centralpark4804@gmail.com that read, "for a thrill try out bumpfire ar's with a 100
2 round magazine." Investigators believe these communications may have been related to
3 the eventual attack that occurred at the Mandalay Bay in Las Vegas.

4 13. Your Affiant believes the requested search warrants will yield significant
5 information from Microsoft such as STEPHEN PADDOCK's and MARILOU DANLEY's
6 contact lists, email messages content, IP address usage, photographs, third-party
7 applications associated with the account, and more, which may constitute evidence of
8 the planning of the attack and potentially identify other participants in the attack.
9 Ultimately, your Affiant strongly believes the requested information will lead
10 investigators to determine the full scope of STEPHEN PADDOCK's plan and MARILOU
11 DANLEY's possible involvement.

12 14. Investigators have previously sought and obtained a search warrant to
13 examine the contents of both Target Accounts 1 and 2. After execution of that warrant,
14 however, it became apparent and was confirmed with Microsoft that Microsoft was
15 refusing to provide data related to/contained in the OneDrive online storage files for
16 either account. Microsoft indicated to investigators that it did not believe such
17 information was encompassed by the items to be produced that were specified in the
18 original warrant. Investigators believe therefore that there is additional evidence
19 Microsoft currently possesses that relates to the OneDrive online storage service, as well
20 as potentially in a suite of other online services that Microsoft offers, including Office
21 365, Windows Live Mail, Windows Live Writer, Windows Photo Gallery, Windows Live
22 Messenger, Microsoft Family Safety, and Microsoft Outlook Hotmail Connector. Thus,
23
24

1 your Affiant seeks more specific authorization to seize and search the OneDrive and
2 other service data specified in Attachment B of the instant warrant application.

3 RELEVANT TECHNICAL TERMS

4 15. The following non-exhaustive list of definitions applies to this Affidavit and
5 the Attachments to this Affidavit:

6 a. The "Internet" is a worldwide network of computer systems operated
7 by governmental entities, corporations, and universities. In order to access the Internet,
8 an individual computer user must subscribe to an access provider, which operates a host
9 computer system with direct access to the Internet. The World Wide Web is a
10 functionality of the Internet which allows users of the Internet to share information.

11 b. "Internet Service Providers" are companies that provide access to the
12 Internet. ISPs can also provide other services for their customers including website
13 hosting, email service, remote storage, and co-location of computers and other
14 communications equipment. ISPs offer different ways to access the Internet including
15 telephone-based (dial-up), broadband-based access via a digital subscriber line (DSL) or
16 cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge
17 a fee based upon the type of connection and volume of data (bandwidth). Many ISPs
18 assign each subscriber an account name, such as a user name, an email address, and an
19 email mailbox, and the subscriber typically creates a password for his/her account.

20 c. "ISP Records" are records maintained by ISPs pertaining to their
21 subscribers (regardless of whether those subscribers are individuals or entities). These
22 records may include account application information, subscriber and billing information,
23 account access information (often in the form of log files), emails, information concerning
24

1 content uploaded and/or stored on the ISP's servers, and other information, which may
2 be stored both in computer data format and in written or printed record format. ISPs
3 reserve and/or maintain computer disk storage space on their computer system for their
4 subscribers' use. This service by ISPs allows for both temporary and long-term storage
5 of electronic communications and many other types of electronic data and files.

6 d. "Online service providers" (also referred to here as "service
7 providers") are companies that provide online services such as email, chat or instant
8 messaging, word processing applications, spreadsheet applications, presentation
9 applications similar to PowerPoint, online calendar, photo storage and remote storage
10 services. Sometimes they also can provide web hosting, remote storage, and co-location
11 of computers and other communications equipment. Typically, each service provider
12 assigns each subscriber an account name, such as a user name or screen name and the
13 subscriber typically creates a password for his/her account.

14 e. "Computer," as used herein, is defined as "an electronic, magnetic,
15 optical, electrochemical, or other high speed data processing device performing logical or
16 storage functions, and includes any data storage facility or communications facility
17 directly related to or operating in conjunction with such device."

18 f. A "server" is a centralized computer that provides services for other
19 computers connected to it via a network. The other computers attached to a server are
20 sometimes called "clients." For example, in a large company, it is common for individual
21 employees to have client computers at their desktops. When the employees access their
22 email, or access files stored on the network itself, those files are pulled electronically
23 from the server, where they are stored, and are sent to the client's computer via the
24

1 network. Notably, servers can be physically stored in any location: it is not uncommon
2 for a network's server to be located hundreds (and even thousands) of miles away from
3 the client computers.

4 g. "Internet Protocol address," or "IP address," refers to a unique
5 number used by a computer to access the Internet. IP addresses can be dynamic,
6 meaning that the Internet Service Provider (ISP) assigns a different unique number to
7 a computer every time it accesses the Internet. IP addresses might also be static, that
8 is, an ISP assigns a user's computer a particular IP address which is used each time the
9 computer accesses the Internet.

10 h. The term "domain" refers to a word used as a name for computers,
11 networks, services, etc. A domain name typically represents a website, a server computer
12 that hosts that website, or even some computer (or other digital device) connected to the
13 internet. Essentially, when a website (or a server computer that hosts that website) is
14 connected to the internet, it is assigned an IP address. Because IP addresses are difficult
15 for people to remember, domain names are instead used because they are easier to
16 remember than IP addresses. Domain names are formed by the rules and procedures of
17 the Domain Name System (DNS). A common top level domain under these rules is ".com"
18 for commercial organizations, ".gov" for the United States government, and ".org" for
19 organizations. For example, www.usdoj.gov is the domain name that identifies a server
20 used by the U.S. Department of Justice, and which uses IP address of 149.101.46.71.

21 i. "Web hosting services" maintain server computers connected to the
22 Internet. Their customers use those computers to operate websites on the Internet.
23 Customers of web hosting companies place files, software code, databases, and other data
24

1 on servers. To do this, customers typically connect from their own computers to the
2 server computers across the Internet.

3 j. The term "WhoIs" lookup refers to a search of a publicly available
4 online database that lists information provided when a domain is registered or when an
5 IP address is assigned.

6 k. The terms "communications," "records," "documents," "programs," or
7 "materials" include all information recorded in any form, visual or aural, and by any
8 means, whether in handmade form (including, but not limited to, writings, drawings,
9 paintings), photographic form (including, but not limited to, pictures or videos), or
10 electrical, electronic or magnetic form, as well as digital data files. These terms also
11 include any applications (i.e. software programs). These terms expressly include, among
12 other things, emails, instant messages, chat logs, correspondence attached as to emails
13 (or drafts), calendar entries, buddy lists.

14 l. "Chat" is usually a real time electronic communication between two
15 or more individuals. Unlike email, which is frequently sent, then read and responded to
16 minutes, hours, or even days later, chats frequently involve an immediate conversation
17 between individuals, similar to a face-to-face conversation. Nearly all chat programs are
18 capable of saving the chat transcript, to enable users to preserve a record of the
19 conversation. By default, some chat programs have this capability enabled, while others
20 do not. Many popular web-based email providers, like Microsoft and Microsoft, provide
21 chat functionality as part of the online services they provide to account holders.

22 ///

23 ///

24

1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8
9
0
1
2
3
4

15
16
17
18
19
20
21
22
23
24

24

1 18. In general, when a subscriber receives an email, it is typically stored in the
2 subscriber's "mail box" on that service provider's servers until the subscriber deletes the
3 Email. If the subscriber does not delete the message, the message (and any attachments)
4 can remain on that service provider's servers indefinitely.

5 19. Similarly, when the subscriber sends an email, it is initiated at the
6 subscriber's computer, transferred via the Internet to the service provider's servers, and
7 then transmitted to its end destination. That service provider often saves a copy of the
8 email sent. Unless the sender of the email specifically deletes the Email from the
9 provider's server, the email can remain on the system indefinitely.

10 20. A sent or received email typically includes the content of the message,
11 source and destination addresses, the date and time at which the email was sent, and
12 the size and length of the email. If an email user writes a draft message but does not
13 send it, that message may also be saved by that service provider, but may not include all
14 of these categories of data.

15 21. Just as a computer on a desk can be used to store a wide variety of files, so
16 can online accounts, such as the accounts subject to this application. First, subscribers
17 can store many types of files as attachments to emails in online accounts. Second,
18 because service providers provide the services listed above (e.g. word processing,
19 spreadsheets, pictures), subscribers who use these services usually store documents on
20 servers maintained and/or owned by service providers. Thus, these online accounts often
21 contain documents such as pictures, audio or video recordings, logs, spreadsheets,
22 applications and other files.

1 22. Reviewing files stored in online accounts raises many of the same
2 difficulties as with reviewing files stored on a local computer. For example, based on my
3 training, my experience and this investigation, I know that subscribers of these online
4 services can conceal their activities by altering files before they upload them to the online
5 service. Subscribers can change file names to more innocuous sounding names (e.g.
6 renaming "FraudRecords.doc" to "ChristmasList.doc"), they can change file extensions
7 to make one kind of file appear like a different type of file (e.g. changing the spreadsheet
8 "StolenCreditProfiles.xls" to "FamilyPhoto.jpg" to appear to be a picture file, where the
9 file extension ".xls" denotes an Excel spreadsheet file and ".jpg" a JPEG format image
10 file), or they can change the times and dates a file was last accessed or modified by
11 changing a computer's system time/date and then uploading that file to the Online
12 Accounts. Thus, to detect any files that the subscriber may have concealed, agents will
13 need to review all of the files in the Target Accounts; they will, however, only seize the
14 items that the Court authorizes to be seized. Similarly, subscribers can conceal their
15 activities by encrypting files. Thus, these files may need to be decrypted to detect
16 whether it constitutes an Item to be Seized.

17 23. I also believe that people engaged in crimes such as the one described
18 herein often use online accounts because they give people engaged in these crimes a way
19 to easily communicate with other co-conspirators. Moreover, online accounts are easily
20 concealed from law enforcement. Unlike physical documents, electronic documents can
21 be stored in a physical place far away, where they are less likely to be discovered.

22 24. Service providers typically retain certain transactional information about
23 the creation and use of each account on their systems. This information can include the
24

1 date on which the account was created, the length of service, records of log-in (i.e.,
2 session) times and durations, the types of service utilized, the status of the account
3 (including whether the account is inactive or closed), the methods used to connect to the
4 account (such as logging into the account via websites controlled by the Service
5 Provider), and other log files that reflect usage of the account. In addition, service
6 providers often have records of the Internet Protocol address ("IP address") used to
7 register the account and the IP addresses associated with particular logins to the
8 account. Because every device that connects to the Internet must use an IP address, IP
9 address information can help to identify which computers or other devices were used to
10 access the online account.

11 25. In some cases, subscribers will communicate directly with a service
12 provider about issues relating to the account, such as technical problems, billing
13 inquiries, or complaints from or about other users. Service providers typically retain
14 records about such communications, including records of contacts between the user and
15 the provider's support services, as well records of any actions taken by the provider or
16 user as a result of the communications.

17 26. In my training and experience, evidence of who was using an online account
18 may be found in address books, contact or buddy lists, emails in the account, and pictures
19 and files, whether stored as attachments or in the suite of the service provider's online
20 applications. Therefore, the computers of the Service Providers are likely to contain
21 stored electronic communications (including retrieved and un-retrieved email for their
22 subscribers) and information concerning subscribers and their use of the provider's
23
24

1 services, such as account access information, email transaction information, documents,
2 pictures, and account application information.

3 27. Microsoft maintains and offers its users the use of OneDrive. OneDrive is
4 a file-hosting service operated by Microsoft as part of its suite of online services. It allows
5 users to store files as well as other personal data like Windows settings or BitLocker
6 recovery keys in the cloud. Files can be synced to a PC and accessed from a web browser
7 or a mobile device, as well as shared publicly or with specific people. OneDrive offers 5
8 gigabytes of storage space free of charge; additional storage can be added either
9 separately or through subscriptions to other Microsoft services including Office 365 and
10 Groove Music.

11 28. Microsoft offers additional services that may be accessed in relation to and
12 share associated information with a user's email account, including: Office 365, Windows
13 Live Mail, Windows Live Writer, Windows Photo Gallery, Windows Live Messenger,
14 Microsoft Family Safety, and Microsoft Outlook Hotmail Connector.

15 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

16 29. Your Affiant anticipates executing these warrants under the Electronic
17 Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and
18 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government
19 copies of the records and other information (including the content of communications)
20 particularly described in Section I of Attachment "B." Upon receipt of the information
21 described in Section I of Attachment "B," government-authorized persons will review
22 that information to locate the items described in Section II of Attachment "B."
23
24

1 CONCLUSION

2 30. Based on the forgoing, I request that the Court issue the proposed search
3 warrant. This Court has jurisdiction to issue the requested warrant because it is "a court
4 of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A)
5 & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has
6 jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to
7 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the
8 service or execution of this warrant.

9 REQUEST FOR SEALING

10 31. I further request that the Court order that all papers in support of this
11 application, including the affidavit and search warrant, be sealed until further order of
12 the Court. These documents discuss an ongoing criminal investigation that is neither
13 public nor known to all of the targets of the investigation. Accordingly, there is good
14 cause to seal these documents because their premature disclosure may seriously
15 jeopardize that investigation.

16
17 Respectfully Submitted,

18 /s/
19 Zachary C. McKinney, Special Agent
Federal Bureau of Investigation

20 SWORN TO AND SUBSCRIBED
21 before me this 13th day of October 2017.

22 NANCY J. KOPPE
23 UNITED STATES MAGISTRATE JUDGE

I hereby attest and certify on 10/13/17
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.

24 By [Signature] Deputy Clerk
NANCY J. KOPPE
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "A-1"

ONLINE ACCOUNT TO BE SEARCHED

This warrant applies to information associated with the Microsoft email account centralpark1@live.com (the "Target Account 1") from inception to present, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.

1 ATTACHMENT "A-2"

2 ONLINE ACCOUNT TO BE SEARCHED

3 This warrant applies to information associated with the Microsoft email account
4 marilouroses@live.com (the "Target Account 2") from inception to present, which is
5 stored at premises owned, maintained, controlled, or operated by Microsoft Corporation,
6 headquartered at 1 Microsoft Way, Redmond, Washington, 98052.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachments A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachments A-1 and A-2 from account inception to present:

- a. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any OneDrive accounts associated with or assigned to Target Accounts 1 and 2.
- b. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Office 360 accounts associated with or assigned to Target Accounts 1 and 2.
- c. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Microsoft Family Safety accounts or services associated with or assigned to Target Accounts 1 and 2.
- d. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Writer accounts or services associated with or assigned to Target Accounts 1 and 2.
- e. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Mail accounts or services associated with or assigned to Target Accounts 1 and 2.
- f. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Photo Gallery accounts or services associated with or assigned to Target Accounts 1 and 2.
- g. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Messenger accounts or services associated with or assigned to Target Accounts 1 and 2.

1 II. Information to be seized by the United States

2 After reviewing all information described in Section I, the United States will seize
3 evidence of violations of Title 18, United States Code Sections 32(a)
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
5 International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of
6 Firearms by Non Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject
7 Offenses") that occur in the form of the following, from account inception to present:

- 8 a. Communications, transactions and records that may establish ownership
9 and control (or the degree thereof) of the Target Account, including address
10 books, contact or buddy lists, bills, invoices, receipts, registration records,
11 bills, correspondence, notes, records, memoranda, telephone/address books,
12 photographs, video recordings, audio recordings, lists of names, records of
13 payment for access to newsgroups or other online subscription services, and
14 attachments to said communications, transactions and records.
- 15 b. Communications, transactions and records to/from persons who may be co-
16 conspirators of the Subject Offenses, or which may identify co-conspirators.
- 17 c. Communications, transactions and records which may show motivation to
18 commit the Subject Offenses.
- 19 d. Communications, transactions and records that relate to the Subject
20 Offenses.
- 21 e. The terms "communications," "transactions," "records," "documents,"
22 "programs," or "materials" include all information recorded in any form,
23 visual or aural, and by any means, whether in handmade form (including,
24 but not limited to, writings, drawings, paintings), photographic form
25 (including, but not limited to, pictures or videos), or electrical, electronic or
26 magnetic form, as well as digital data files. These terms also include any
27 applications (i.e. software programs). These terms expressly include, among
28 other things, Emails, instant messages, chat logs, correspondence attached
29 as to Emails (or drafts), calendar entries, buddy lists.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "C"

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

1 5. The search procedures utilized for this review are at the sole discretion of
2 the investigating and prosecuting authorities, and may include the following techniques
(the following is a non-exclusive list, as other search procedures may be used):

3 a. examination of all of the data contained in the Search Warrant Data to view
4 the data and determine whether that data falls within the items to be seized as set forth
herein;

5 b. searching for and attempting to recover from the Search Warrant Data any
6 deleted, hidden, or encrypted data to determine whether that data falls within the list
7 of items to be seized as set forth herein (any data that is encrypted and unreadable will
8 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

9 c. surveying various file directories and the individual files they contain;

10 d. opening files in order to determine their contents;

11 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

12 f. scanning storage areas;

13 g. performing keyword searches through all electronic storage areas to
14 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A1 and A2; and/or

15 h. performing any other data analysis technique that may be necessary to
16 locate and retrieve the evidence described in Attachment B, Section II.

17 Return and Review Procedures

18 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
19 part:

20 (e) Issuing the Warrant.

21 (2) Contents of the Warrant.

22 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
23 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
24 be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
4 copying of electronically stored information. Unless otherwise specified, the warrant
5 authorizes a later review of the media or information consistent with the warrant. The
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
7 on-site copying of the media or information, and not to any later off-site copying or
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare
9 and verify an inventory of any property seized. . . . In a case involving the seizure of
10 electronic storage media or the seizure or copying of electronically stored information,
11 the inventory may be limited to describing the physical storage media that were seized
12 or copied. The officer may retain a copy of the electronically stored information that was
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
15 of the warrant, an agent is required to file an inventory return with the Court, that is,
16 to file an itemized list of the property seized. Execution of the warrant begins when
17 the United States serves the warrant on the named custodian; execution is complete
18 when the custodian provides all Search Warrant Data to the United States. Within
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be
20 filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
19 which the electronically stored information must be seized after the issuance of the
20 warrant and copied after the execution of the warrant, not the "later review of the media
21 or information" seized, or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
23 may be limited to a description of the "physical storage media" into which the Search
24 Warrant Data that was seized was placed, not an itemization of the information or data
stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
2 purposes of the investigation. The government proposes that the original storage media
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search
4 Warrant Data be retained by the government.
5
6 e. If the person from whom any Search Warrant Data was seized requests the return
7 of any information in the Search Warrant Data that is not set forth in Attachment B,
8 Section II, that information will be copied onto appropriate media and returned to the
9 person from whom the information was seized.
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "A-1"

ONLINE ACCOUNT TO BE SEARCHED

This warrant applies to information associated with the Microsoft email account centralpark1@live.com (the "Target Account 1") from inception to present, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachments A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachments A-1 and A-2 from account inception to present:

- a. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any OneDrive accounts associated with or assigned to Target Accounts 1 and 2.
- b. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Office 360 accounts associated with or assigned to Target Accounts 1 and 2.
- c. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Microsoft Family Safety accounts or services associated with or assigned to Target Accounts 1 and 2.
- d. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Writer accounts or services associated with or assigned to Target Accounts 1 and 2.
- e. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Mail accounts or services associated with or assigned to Target Accounts 1 and 2.
- f. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Photo Gallery accounts or services associated with or assigned to Target Accounts 1 and 2.
- g. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Messenger accounts or services associated with or assigned to Target Accounts 1 and 2.

1 II. Information to be seized by the United States

2 After reviewing all information described in Section I, the United States will seize
3 evidence of violations of Title 18, United States Code Sections 32(a)
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
5 International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of
6 Firearms by Non-Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject
7 Offenses") that occur in the form of the following, from account inception to present:

- 8 a. Communications, transactions and records that may establish ownership
9 and control (or the degree thereof) of the Target Account, including address
10 books, contact or buddy lists, bills, invoices, receipts, registration records,
11 bills, correspondence, notes, records, memoranda, telephone/address books,
12 photographs, video recordings, audio recordings, lists of names, records of
13 payment for access to newsgroups or other online subscription services, and
14 attachments to said communications, transactions and records.
- 15 b. Communications, transactions and records to/from persons who may be co-
16 conspirators of the Subject Offenses, or which may identify co-conspirators.
- 17 c. Communications, transactions and records which may show motivation to
18 commit the Subject Offenses.
- 19 d. Communications, transactions and records that relate to the Subject
20 Offenses.
- 21 e. The terms "communications," "transactions," "records," "documents,"
22 "programs," or "materials" include all information recorded in any form,
23 visual or aural, and by any means, whether in handmade form (including,
24 but not limited to, writings, drawings, paintings), photographic form
25 (including, but not limited to, pictures or videos), or electrical, electronic or
26 magnetic form, as well as digital data files. These terms also include any
27 applications (i.e. software programs). These terms expressly include, among
28 other things, Emails, instant messages, chat logs, correspondence attached
29 as to Emails (or drafts), calendar entries, buddy lists.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "C"

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

1 5. The search procedures utilized for this review are at the sole discretion of
2 the investigating and prosecuting authorities, and may include the following techniques
3 (the following is a non-exclusive list, as other search procedures may be used):

4 a. examination of all of the data contained in the Search Warrant Data to view
5 the data and determine whether that data falls within the items to be seized as set forth
6 herein;

7 b. searching for and attempting to recover from the Search Warrant Data any
8 deleted, hidden, or encrypted data to determine whether that data falls within the list
9 of items to be seized as set forth herein (any data that is encrypted and unreadable will
10 not be returned unless law enforcement personnel have determined that the data is not
11 (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
12 (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

13 c. surveying various file directories and the individual files they contain;

14 d. opening files in order to determine their contents;

15 e. using hash values to narrow the scope of what may be found. Hash values
16 are under- inclusive, but are still a helpful tool;

17 f. scanning storage areas;

18 g. performing keyword searches through all electronic storage areas to
19 determine whether occurrences of language contained in such storage areas exist that
20 are likely to appear in the evidence described in Attachment A1 and A2; and/or

21 h. performing any other data analysis technique that may be necessary to
22 locate and retrieve the evidence described in Attachment B, Section II.

23 Return and Review Procedures

24 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
25 part:

26 (e) Issuing the Warrant.

27 (2) Contents of the Warrant.

28 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
29 device warrant, the warrant must identify the person or property to be searched, identify
30 any person or property to be seized, and designate the magistrate judge to whom it must
31 be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
4 copying of electronically stored information. Unless otherwise specified, the warrant
5 authorizes a later review of the media or information consistent with the warrant. The
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
7 on-site copying of the media or information, and not to any later off-site copying or
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare
9 and verify an inventory of any property seized. . . . In a case involving the seizure of
10 electronic storage media or the seizure or copying of electronically stored information,
11 the inventory may be limited to describing the physical storage media that were seized
12 or copied. The officer may retain a copy of the electronically stored information that was
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
15 of the warrant, an agent is required to file an inventory return with the Court, that is,
16 to file an itemized list of the property seized. Execution of the warrant begins when
17 the United States serves the warrant on the named custodian; execution is complete
18 when the custodian provides all Search Warrant Data to the United States. Within
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be
20 filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
19 which the electronically stored information must be seized after the issuance of the
20 warrant and copied after the execution of the warrant, not the "later review of the media
21 or information" seized, or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
23 may be limited to a description of the "physical storage media" into which the Search
24 Warrant Data that was seized was placed, not an itemization of the information or data
stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
2 purposes of the investigation. The government proposes that the original storage media
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return
5 of any information in the Search Warrant Data that is not set forth in Attachment B,
6 Section II, that information will be copied onto appropriate media and returned to the
7 person from whom the information was seized.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

1 STEVEN W. MYHRE
Acting United States Attorney
2 District of Nevada
Cristina D. Silva
3 Patrick Burns
Assistant United States Attorneys
4 501 Las Vegas Blvd. South, Ste. 1100
Las Vegas, Nevada 89101
5 Telephone: (702) 388-6336
Fax (702) 388-6698
6 CSilva@usa.doi.gov
john.p.burns@usdoj.gov

7 *Representing the United States of America*

8 UNITED STATES DISTRICT COURT
9 DISTRICT OF NEVADA

10 -oOo-

11 IN THE MATTER OF THE SEARCH OF:

Magistrate No. 17-mj-973-NJK

12 THE PREMISES KNOWN AS:
13 1372 BABBLING BROOK COURT,
MESQUITE, COUNTY OF CLARK,
STATE OF NEVADA.

AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT

(Under Seal)

15 STATE OF NEVADA)
16) ss:
17 COUNTY OF CLARK)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

18 1. I, Christopher W. McPeak, Special Agent, Federal Bureau of Investigation (FBI),
19 having been duly sworn, hereby depose and say:

20 2. Your Affiant is a Special Agent with the FBI currently assigned to the Las Vegas,
21 Nevada Division and has been so employed for over eight years. Prior to this he was employed
22 for over five years as a Deputy Sheriff and Detective with the Orange County, Florida Sheriff's
23 Office. As an FBI Agent, your Affiant is assigned to the FBI's Las Vegas Safe Streets Task Force
24 (LVSSTF) and is responsible for investigating a variety of violent crimes, to include bank
25

1 robbery, kidnapping, extortion, robbery, carjackings, assaults and murders of federal officers,
2 racketeering related violent offenses, as well as long-term investigations into the activities and
3 operations of career criminals, criminal enterprises, drug trafficking organizations, and violent
4 street gangs. Your Affiant has experience in conducting criminal investigations, including the
5 investigation of criminal groups and conspiracies as well as the collection of evidence and the
6 identification and use of witnesses.

7 3. The facts in this affidavit are derived from your Affiant's personal observations,
8 his training and experience, and information obtained from other agents, detectives, and
9 witnesses. This affidavit is intended to show merely that there is sufficient probable cause for
10 the requested warrant and does not set forth all of the Affiant's knowledge about this matter.

11 PREMISES TO BE SEARCHED

12 4. The proposed search warrant seeks authorization to search the premises identified
13 as 1372 Babbling Brook Court, Mesquite, Clark County, Nevada (hereinafter referred to as the
14 "subject premises"), more fully described in Attachment "A" (attached hereto and incorporated
15 herein by reference).

16 REQUEST FOR SEARCH WARRANT

17 5. Based on your Affiant's training and experience and the facts as set forth in this
18 affidavit, there is probable cause to believe that violations of, *inter alia*:

- 19 a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C. § 32(a);
- 20 b. Violence at an International Airport - 18 U.S.C. § 37(a)(2);
- 21 c. Unlawful Interstate Transport/Delivery of Firearms by Non-Federal
22 Firearms Licensee - 18 U.S.C. § 922(a)(3) and (5); and
- 23 d. Aiding and Abetting - 18 U.S.C. § 2,

24 (hereinafter referred to as the "subject offenses") have been committed by Stephen Paddock and
25 others yet unknown; and this affidavit is made in support of an application for a search warrant

1 to search the subject premises for evidence and instrumentalities of the subject offenses, more
2 fully described in Attachment "B" (attached hereto and incorporated herein by reference).

3 BACKGROUND OF INVESTIGATION

4 6. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music festival,
5 was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At approximately 10:08
6 p.m., the Las Vegas Metropolitan Police Department (LVMPD) received calls reporting shots
7 had been fired at the concert and multiple victims were struck (the "attack"). LVMPD
8 determined the shots were coming from Rooms 134 and 135 on the 32nd floor of the Mandalay
9 Bay Resort and Casino, located due west of the festival grounds at 3950 South Las Vegas
10 Boulevard, Las Vegas, Nevada. These rooms are an elevated position which overlooks the
11 concert venue. Witness statements and video footage captured during the attack indicates that
12 the weapons being used were firing in a fully-automatic fashion.

13 7. LVMPD officers ultimately made entry into the room and located an individual
14 later identified as Stephen Paddock. Paddock was deceased from an apparent self-inflicted
15 gunshot wound.

16 8. Paddock's Nevada driver's license was located in the Mandalay Bay hotel room
17 with Paddock, and both hotel rooms were registered in his name. A player's club card in name
18 of Marilou Danley was located in Paddock's room, and the card returned to the address located
19 on Babbling Brook Court in Mesquite, Nevada. FBI Agents located Danley, who was traveling
20 outside the United States at the time of the shooting. It was ultimately determined that Danley
21 resided with Paddock at the Babbling Brook address.

22 9. On October 2, 2017, local search warrants were obtained and executed on
23 Paddock's Mandalay Bay hotel rooms, Paddock's vehicle parked in the Mandalay Bay parking
24
25

1 garage, and two Nevada residences owed by Paddock: 1372 Babbling Brook Court¹, and 1735 Del
2 Webb Parkway, Reno, Nevada. Pursuant to those searches, Officers and Agents found over 20
3 firearms, hundreds of rounds of unfired ammunition (much of it in preloaded high-capacity
4 magazines), range finding devices, several suitcases (some partially full of pre-loaded high
5 capacity magazines) a set of body armor, an apparent homemade gas mask, and hundreds of
6 spent cartridge cases in the Mandalay Bay hotel rooms, in close proximity to Paddock's body.
7 Over a thousand rounds of rifle ammunition and a significant amount of explosive precursor
8 material was found in Paddock's vehicle (specifically the binary explosive brand-named
9 Tannerite). Additional explosive precursor material, approximately 18 firearms, and over 1,000
10 rounds of ammunition were located at the Mesquite residence. A large quantity of ammunition
11 and multiple firearms were recovered from the Reno residence.

12 10. Immediately following the shooting, an extensive investigation was commenced
13 which is currently being conducted jointly by LVMPD and the FBI, with the substantial support
14 of numerous state, local and federal law enforcement agencies. As of this date, 58 people have
15 been identified to have been killed in Paddock's attack and over 500 were reportedly injured.
16 The preliminary reviews of the crime scenes in and around the Mandalay Bay led investigators
17 to determine that in addition to firing upon the crowds at the festival grounds, Paddock also
18 fired several high-caliber rifle shots at large fuel tanks within the property line of the McCarran
19 International airport property. Multiple bullet impacts were located on the tank, which
20 investigators believe was an attempt by Paddock to explode the tanks.

21 11. As the investigation progressed, investigators learned that Paddock planned the
22 attack meticulously and took many methodical steps to avoid detection of his plot and to thwart
23 the eventual law enforcement investigation that would follow. The steps included the apparent
24

25 ¹ The search warrant for this location was approved by [REDACTED]
[REDACTED] A copy of that search warrant is attached hereto as Exhibit 1.

1 destruction and/or concealment of digital storage media and the use of anonymously attributed
2 communications devices. Based on your Affiant's training and experience, it is his belief that the
3 methodical nature of the planning employed by Paddock, coupled with his efforts to undermine
4 the preceding investigation, are factors indicative of a level of sophistication which is commonly
5 found in mass casualty events such as this. However, your Affiant notes that this finding was
6 not fully-developed in this case until several days into the investigation, after the subject
7 premises had been searched in the hours immediately after the attack unfolded.

8 12. The investigation has also revealed that Paddock may have been treated for yet
9 unidentified medical conditions, and that he spent significant time and expense prior to the
10 attack purchasing and caching the weapons and other instrumentalities he used in the shooting.
11 Some of these items included glass cutters, suitcases and a pre-paid cellular telephone. This
12 cache included a substantial amount of ammunition, "Tannerite,"² glass cutters, numerous
13 suitcases, and at least one identified pre-paid cellular telephone.

14 13. Investigators are currently conducting analysis of available financial records. To
15 date, this analysis has revealed that Paddock made the purchases of items used in the attack
16 throughout the last approximately 12 months. A large portion of the ammunition and firearms
17 accessory purchases appear to have been made through Internet based retailers. Law
18 enforcement continues to investigate the sourcing of purchases made by Paddock preceding the
19 attack.

20 14. Subsequent to her identification as Paddock's companion and co-habitant at the
21 subject premises, Marilou Danely returned to the United States and was thereafter voluntarily
22 interviewed by law enforcement with her attorney present. During the interview, Danley
23 corroborated much of what had been previously deduced by investigators, but she was adamant
24

25 ² Tannerite is the brand name of a commercially available binary explosive commonly used as a reactive
rifle target in shooting sports it can also be a precursor chemical for an improvised explosive devices.

1 that she had no prior inclination of Paddock intentions to conduct the attack. While investigators
2 obtained a DNA buccal swab sample from Danley, she spontaneously stated that her fingerprints
3 would likely be found on Paddock's ammunition because she occasionally participated in loading
4 magazines. Danley has not been arrested and she has agreed to cooperate with investigators.
5 Although, the investigation to date has not produced any conclusive evidence that Danley aided
6 Paddock, had foreknowledge of his plans, or has been deceptive with law enforcement, this aspect
7 of the investigation is still the subject of intensive review. Therefore, your Affiant asserts, for
8 the purposes of this affidavit, that although there is currently no evidence to suggest criminal
9 involvement by Danley, investigators are not yet prepared to rule this possibility out.

10 15. Investigators have reviewed the findings of the initial search of the subject
11 premises and have determined that an additional, more exhaustive search is required. The
12 proposed search would be focused on finding items of evidence or instrumentalities that may
13 have been concealed inside or within the curtilage of the subject premises. In addition, the
14 search will include a more thorough effort to identify any forensic trace evidence that may be
15 located inside or within the curtilage of the subject premises.

16 PROBABLE CAUSE

17 16. Your Affiant believes that probable cause exists for this Court to authorize the
18 proposed search, and that this probable cause is relatively unchanged from the probable cause
19 that existed in the hour after the attack when the initial search was conducted. Additionally,
20 information received from Danley during her interview and further investigation of the crime
21 scene, as well as a fuller understanding of Paddock's mode of planning the attack, lead your
22 Affiant to believe there is probable cause that additional evidence of the subject offenses may be
23 located in the subject residence.


24 17. The primary identified resident of the subject premises, Stephen Paddock, is
25 deceased and as such, no longer holds standing at 1372 Babbling Brook Court. Investigators are

1 currently unable to determine Danley's standing to provide consent to conduct this subsequent
2 search. Therefore, although the FBI might already have all necessary authority to conduct the
3 proposed search, your Affiant is seeking this search warrant out of an abundance of caution to
4 be certain that any search conducted will comply with the Fourth Amendment and other
5 applicable laws.

6 CONCLUSION

7 18. Based upon the aforementioned facts and circumstances, it is your Affiant's
8 opinion that there is probable cause that the subject premises may contain evidence and
9 instrumentalities concerning violations of the subject offenses herein. Your Affiant's training
10 and experience provides the basis for his belief that a search of the subject premises will yield
11 these items. As such, your Affiant seeks this Court's authorization to conduct a search of the
12 subject premises as fully described in Attachment "A" for the items sought to be seized as
13 described in Attachment "B."

14 Respectfully Submitted,

15 
16 _____
17 Christopher W. McPeak, Special Agent
Federal Bureau of Investigation

18 SWORN TO AND SUBSCRIBED
19 before me this 7th day of October, 2017.

20 
21 _____
22 HONORABLE NANCY J. KOPPE
23 UNITED STATES MAGISTRATE JUDGE
24
25

Attachment "A"

Description of Property/Premise to be Searched

1372 Babbling Brook Court
Mesquite, Clark County, Nevada

The subject premises is described as a one story, single family residence of apparent stucco frame construction. The premises are situated in the northeast corner Babbling Brook Court, which is a cul-de-sac. The premises faces approximately southwest and is located approximately 100 feet from the intersection of Babbling Brook Court and Cool Springs Lane. The residence is painted tan and the house numbers "1372" are affixed to the exterior wall facing the street.

Attachment "B"

Particular Items to be Seized

- a. a thorough, microscopic examination and documentation of the subject premises to discover trace evidence, including but not limited to: fingerprints, blood, hair, fibers and other bodily fluid samples;
- b. firearms to include handguns, shotguns and rifles, spent casings or live ammunition for the same, firearm accessories such as magazines or cylinders, firearm cleaning materials, and paperwork associated with the ownership of firearms;
- c. United States and foreign currency, precious metals, jewelry, property deeds and other negotiable financial instruments including: stocks, bonds, securities, cashier's checks, money drafts, and letters of credit;
- d. books, records, receipts, notes, ledgers, personal checks and other papers relating to the transportation, ordering, and purchase of firearms, firearms accessories, ammunition, explosives or explosives precursor materials, or material relating to any ideological extremism;
- e. books, records, invoices, receipts, records of real estate transactions, bank statements and related records, gambling receipts and records, passbooks, money drafts, letters of credit, money orders, bank drafts, and cashier checks, bank checks, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transfer, and/or concealment and /or expenditure of money;
- f. any and all financial, credit card and bank account information including but not limited to bills and payment records, including those relating to the purchase of firearms, firearms accessories, ammunition, explosives, explosives precursor materials, body armor, range finding devices, scopes and other optical devices, glass cutters, and gas masks;
- g. any and all records relating to the medical or psychological/psychiatric treatment of Stephen Paddock or Marilou Danley;
- h. all types of safes and the contents thereof, including but not limited to, wall safes, floor safes, freestanding safes, locked strong boxes, and locked containers;
- i. photographs, including still photos, negatives, video tapes, films, undeveloped film and the contents therein, slides;
- j. cellular telephones address and/or telephone books, digital pagers, address and/or telephone books, Rolodex indices, electronic organizers, and papers reflecting names, addresses, telephone numbers, pager numbers, fax numbers, e-mail addresses, Facebook account information and other contact information related to co-conspirators, financial institutions, and other individuals or businesses with whom a financial relationship exists;

- 1
- 2 k. papers, tickets, notes, receipts, and other items relating to domestic and international travel.
- 3
- 4 l. any and all electronic storage devices, including: computer hard drives and external memory devices such as floppy disks, "thumb drives" (USB electronic storage drives), and compact disk "CD" and/or "DVD" storage devices.³
- 5
- 6 m. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;
- 7
- 8 n. records or other items which evidence ownership or use of computer equipment found in the target location, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;
- 9
- 10 o. any and all records pertaining to the rental of self-storage units and post office boxes;
- 11
- 12 p. chemicals and other compounds which may constitute explosives or explosive precursors; and
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25 q. improvised, commercial or military grade explosive devices, detonators, initiators, any components thereof, or any other weapon of mass destruction.

³ Electronic equipment shall be seized, but not searched. Supplemental search warrant will be requested prior to the searching of seized electronic items.

EXHIBIT 1

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

UNITED STATES DISTRICT COURT

for the
District of Nevada

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
1372 BABBLING BROOK COURT,
MESQUITE, COUNTY OF CLARK, STATE OF NEVADA.

Case No. 2:17-mj-973-NJK

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Nevada
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B

YOU ARE COMMANDED to execute this warrant on or before October 21, 2017 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: 10/17/2017 6:45 pm

City and state: Las Vegas, Nevada

Judge's signature

Printed name and title

Attachment "A"

Description of Property/Premise to be Searched

1372 Babbling Brook Court
Mesquite, Clark County, Nevada

The subject premises is described as a one story, single family residence of apparent stucco frame construction. The premises are situated in the northeast corner Babbling Brook Court, which is a cul-de-sac. The premises faces approximately southwest and is located approximately 100 feet from the intersection of Babbling Brook Court and Cool Springs Lane. The residence is painted tan and the house numbers "1372" are affixed to the exterior wall facing the street.

Attachment "B"

Particular Items to be Seized

- a. a thorough, microscopic examination and documentation of the subject premises to discover trace evidence, including but not limited to: fingerprints, blood, hair, fibers and other bodily fluid samples;
- b. firearms to include handguns, shotguns and rifles, spent casings or live ammunition for the same, firearm accessories such as magazines or cylinders, firearm cleaning materials, and paperwork associated with the ownership of firearms;
- c. United States and foreign currency, precious metals, jewelry, property deeds and other negotiable financial instruments including: stocks, bonds, securities, cashier's checks, money drafts, and letters of credit;
- d. books, records, receipts, notes, ledgers, personal checks and other papers relating to the transportation, ordering, and purchase of firearms, firearms accessories, ammunition, explosives or explosives precursor materials, or material relating to any ideological extremism;
- e. books, records, invoices, receipts, records of real estate transactions, bank statements and related records, gambling receipts and records, passbooks, money drafts, letters of credit, money orders, bank drafts, and cashier checks, bank checks, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transfer, and/or concealment and /or expenditure of money;
- f. any and all financial, credit card and bank account information including but not limited to bills and payment records, including those relating to the purchase of firearms, firearms accessories, ammunition, explosives, explosives precursor materials, body armor, range finding devices, scopes and other optical devices, glass cutters, and gas masks;
- g. any and all records relating to the medical or psychological/psychiatric treatment of Stephen Paddock or Marilou Danley;
- h. all types of safes and the contents thereof, including but not limited to, wall safes, floor safes, freestanding safes, locked strong boxes, and locked containers;
- i. photographs, including still photos, negatives, video tapes, films, undeveloped film and the contents therein, slides;
- j. cellular telephones address and/or telephone books, digital pagers, address and/or telephone books, Rolodex indices, electronic organizers, and papers reflecting names, addresses, telephone numbers, pager numbers, fax numbers, e-mail addresses, Facebook account information and other contact information related to co-conspirators, financial institutions, and other individuals or businesses with whom a financial relationship exists;

- 1 k. papers, tickets, notes, receipts, and other items relating to domestic and
2 international travel.
- 3 l. any and all electronic storage devices, including: computer hard drives and
4 external memory devices such as floppy disks, "thumb drives" (USB electronic
storage drives), and compact disk "CD" and/or "DVD" storage devices.³
- 5 m. records evidencing occupancy or ownership of the premises described above,
6 including, but not limited to, utility and telephone bills, mail envelopes, or
addressed correspondence;
- 7 n. records or other items which evidence ownership or use of computer equipment
8 found in the target location, including, but not limited to, sales receipts, bills for
Internet access, and handwritten notes;
- 9 o. any and all records pertaining to the rental of self-storage units and post office
boxes;
- 10 p. chemicals and other compounds which may constitute explosives or explosive
11 precursors; and
- 12 q. improvised, commercial or military grade explosive devices, detonators, initiators,
13 any components thereof, or any other weapon of mass destruction.
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

25 ³ Electronic equipment shall be seized, but not searched. Supplemental search warrant will be requested
prior to the searching of seized electronic items.



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

FILED

2017 OCT -3 PM 3:59

U.S. MAGISTRATE JUDGE

BY _____

STEVEN W. MYHRE
Acting United States Attorney
NICHOLAS D. DICKINSON
Assistant United States Attorney
District of Nevada
Nevada Bar No. 12940
501 Las Vegas Boulevard South, Suite 1100
Las Vegas, Nevada 89101
PHONE: (702) 388-6336
NDickinson@usdoj.gov

Counsel for the United States

**UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA**

-oOo-

IN THE MATTER OF SEARCH OF
INFORMATION ASSOCIATED WITH
INSTAGRAM ACCOUNTS STORED AT
PREMISES CONTROLLED BY
FACEBOOK CORPORATION:

stephenpaddock47 A1

Magistrate No. _____

2:17-mj-00958-VCF

AFFIDAVIT

(Under Seal)

IN THE MATTER OF SEARCH OF
INFORMATION ASSOCIATED WITH
INSTAGRAM ACCOUNTS STORED AT
PREMISES CONTROLLED BY
FACEBOOK CORPORATION:

Mariloudanley A2

Magistrate No. _____

2:17-mj-00959-VCF

AFFIDAVIT

(Under Seal)

IN THE MATTER OF SEARCH OF
INFORMATION ASSOCIATED WITH
INSTAGRAM ACCOUNTS STORED AT
PREMISES CONTROLLED BY
FACEBOOK CORPORATION:

Mariloudanley A3

Magistrate No. _____

2:17-mj-00960-VCF

AFFIDAVIT

(Under Seal)

1 IN THE MATTER OF SEARCH OF
2 INFORMATION ASSOCIATED WITH
3 INSTAGRAM ACCOUNTS STORED AT
4 PREMISES CONTROLLED BY
5 FACEBOOK CORPORATION:

6 Mariloudanleypaddock A4

7 IN THE MATTER OF SEARCH OF
8 INFORMATION ASSOCIATED WITH
9 INSTAGRAM ACCOUNTS STORED AT
10 PREMISES CONTROLLED BY
11 FACEBOOK CORPORATION:

12 marilou.danley A5

Magistrate No.

2:17-mj-00961-VCF

FILED
2017 OCT -3 PM 3:59
U.S. MAGISTRATE JUDGE
BY (Under Seal)

Magistrate No.

2:17-mj-00962-VCF

AFFIDAVIT

(Under Seal)

10 STATE OF NEVADA)
11) ss:
12 COUNTY OF CLARK)

13 AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

14 I, Heather D. Burton, Special Agent, Federal Bureau of Investigation (FBI), having been duly
15 sworn, hereby depose and say:

16 INTRODUCTION AND AGENT BACKGROUND

17 1. Your Affiant is a Special Agent with the FBI currently assigned to the Las Vegas,
18 Nevada Division. She has been so employed for over three years. Prior to this she, was employed
19 for five years as a United States Probation Officer in Memphis, Tennessee. Your Affiant is
20 currently assigned to FBI Las Vegas Squad 6. Previously, she was assigned to the Las Vegas Safe
21 Streets Task Force (LVSSTF) and was responsible for investigating a variety of violent crimes, to
22 include bank robbery, kidnapping, extortion, robbery, carjacking, assault and murder of Federal
23 Officers, racketeering related violent offenses, as well as long-term investigations into the activities
24 and operations of criminal enterprises, drug trafficking organizations, and violent street gangs.
Your Affiant has experience in conducting criminal investigations, including the investigation of

1 criminal groups and conspiracies as well as the collection of evidence and the identification and use
2 of witnesses.

3 2. Your Affiant makes this affidavit in support of an application for a search warrant for
4 information associated with certain Instagram, LLC (hereinafter "Instagram") user IDs that are
5 stored at premises owned, maintained, controlled, or operated by Facebook Inc. (hereinafter
6 "Facebook"), a social networking company headquartered in Menlo Park, California. The
7 information to be searched is described in the following paragraphs and in Attachment A1, A2, A3,
8 A4, A5 and B. This affidavit is made in support of an application for a search warrant under 18
9 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the
10 government records and other information in its possession, pertaining to the subscriber or customer
11 associated with user IDs. It is submitted that the information sought through the issuance of the
12 requested warrant constitutes evidence of the following offense: Violation of National Firearms Act
13 – Registration of Firearms, Title 26, United States Code, Section 5841.

14 3. The items to be searched are the associated Instagram user ID names as follows:

15 **stephenpaddock47**

16 **mariloudanley**

17 **mariloudanleyy**

18 **mariloudanleypaddock**

19 **marilou.danley**

20 4. Because this affidavit is being submitted for the limited purpose of securing a search
21 warrant, your Affiant has not included each and every fact known to her concerning this
22 investigation. Your Affiant has set forth only those facts that are necessary to establish probable
23 cause for the above listed offense. The information used to support this search warrant was derived
24 from reports of information obtained from witnesses as well as investigation conducted by other

1 Agents and law enforcement officers related to the incident. This affidavit contains information
2 necessary to support probable cause to believe that the criminal offenses described herein were
3 committed by the defendant, STEPHEN PADDOCK (hereinafter "PADDOCK"), and others yet
4 unidentified, and is not intended to include each and every fact and matter observed by your Affiant
5 or known to the Government. Moreover, to the extent this affidavit contains statements by witnesses,
6 those statements are set forth only in part in substance and are intended to accurately convey the
7 information, but not to be verbatim recitations. All noted times are approximate.

8 JURISDICTION

9 5. This Court has jurisdiction to issue the requested warrant because it is "a court of
10 competent jurisdiction" as defined by 18 U.S.C. § 2711 and 18 U.S.C. §§ 2703(a), (b)(1)(A), and
11 (c)(1)(A). Specifically, the Court is a "district court of the United States (including a magistrate
12 judge of such a court) that . . . has jurisdiction over the offense being investigated. . . ." 18 U.S.C. §
13 2711(3)(A)(i), which took place in Las Vegas, Nevada.

14 BACKGROUND CONCERNING INSTAGRAM

15 6. Instagram, which is owned by Facebook, operates a free-access social-networking
16 website of the same name that can be accessed at <http://www.instagram.com>. Instagram allows its
17 users to create their own profile pages, which can include a short biography, a photo of themselves,
18 videos and other information. Users can access Instagram through its website or by using a special
19 electronic application ("app") created by the company that allows users to access the service through
20 a mobile device.

21 7. Instagram permits users to post photos and videos to their profiles on Instagram and
22 otherwise share them with others on Instagram, as well as certain other social-media services,
23 including Flickr, Facebook, and Twitter. When posting or sharing a photo or video on Instagram, a
24 user can add a caption to it, can add various "tags" that can be used to search for the photo or video

1 (e.g., a user may add the tag #vw to a photo so that people interested in Volkswagen vehicles can
2 search for and find the photo), can add location information, and can add other information, as well
3 as apply a variety of "filters" or other visual effects that can be used to modify the look of the posted
4 photos. In addition, Instagram allows users to make comments on posted photos or videos,
5 including photos or video that the user posts or posted by other users of Instagram. Users can also
6 "like" photos.

7 8. Upon creating an Instagram account, an Instagram user must create a unique
8 Instagram username and an account password. This information is collected and maintained by
9 Instagram.

10 9. Instagram asks users to provide basic identity and contact information upon
11 registration and also allows users to provide additional identity information for their user profile.
12 This information may include the user's full name, e-mail address(es), and phone number(s), as well
13 as potentially other personal information provided directly by the user to Instagram. Once an
14 account is created, users may also adjust various privacy and account settings for the account on
15 Instagram. This information is collected and maintained by Instagram.

16 10. Instagram allows users to have "friends," which are other individuals with whom the
17 user can share information without making the information public. Friends on Instagram may come
18 from either contact lists maintained by the user, other third-party social media websites and
19 information, or searches conducted by the user on Instagram profiles. This information is collected
20 and maintained by Instagram.

21 11. Instagram also allows users to "follow" another user, which means that they receive
22 updates about posts made by the other user. Users may also "unfollow" users, that is, stop following
23 them or block them, which prevents the blocked user from following that user.

24 12. Instagram allows users to post and share various types of user content, including

1 photos, videos comments, and other materials. User content that is posted to Instagram or shared
2 through Instagram is collected and maintained by Instagram.

3 13. Instagram users can exchange private messages on Instagram with other users. These
4 messages, which are similar to email messages, are sent to the recipient's "Inbox" on Instagram,
5 which also stores copies of messages sent by the recipient, as well as other information.

6 14. Users on Instagram may also search Instagram for other users or particular types of
7 photos or other content.

8 15. For each user, Instagram also collects and retains information, called "log file"
9 information, every time a user requests access to Instagram, whether through a web page or through
10 an app. Among the log file information that Instagram's servers automatically record is the
11 particular web requests, any Internet Protocol ("IP") address associated with the request, type of
12 browser used, any referencing/exit web pages and associated URLs, pages viewed, dates and times
13 of access, and other information.

14 16. Instagram also collects and maintains "cookies," which are small text files that are
15 placed on a user's computer or mobile device and that allows Instagram to identify the browser or
16 device's accesses to the service.

17 17. Instagram also collects information on the particular devices used to access
18 Instagram. In particular, Instagram may record "device identifiers," which includes data files and
19 other information that may identify the particular electronic device that was used to access
20 Instagram.

21 18. Instagram also collects metadata associated with user content. For example,
22 Instagram collects any "hashtags" associated with user content (i.e., keywords used), "geotags" that
23 mark the location of a photo and which may include latitude and longitude information, comments
24 on photos, and other information.

1 19. Instagram also may communicate with the user, by email or otherwise. Instagram
2 collects and maintains copies of communications between Instagram and the user.

3 20. Based on the information above, the computers of Instagram are likely to contain all
4 the material described above with respect to accounts with the above referenced user IDs, including
5 **stephenpaddock47, mariloudanley, mariloudanleyy, mariloudanleypaddock, and**
6 **marilou.danley**, including stored electronic communications and information concerning
7 subscribers and their use of Instagram, such as account access information, which would include
8 information such as the IP addresses and devices used to access the account, as well as other account
9 information that might be used to identify the actual user or users of the accounts at particular times.

10 **STATEMENT OF PROBABLE CAUSE**

11 21. On the evening of Sunday, October 1, 2017, the Route 91 Harvest, a music festival,
12 was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada 89119. At approximately
13 2208 hours, the Las Vegas Metropolitan Police Department (LVMPD) received calls reporting shots
14 had been fired at the concert and multiple victims were struck. LVMPD determined the shots were
15 coming from Rooms 134 and 135 on the 32nd floor of the Mandalay Bay Resort and Casino, 3950
16 South Las Vegas Boulevard, Las Vegas, Nevada 89119.

17 22. Officers made entry into the room and located an individual later identified as
18 Stephen Paddock, DOB [REDACTED] address 1372 Babbling Brook Court, Mesquite, Nevada 89034.
19 Paddock was deceased from an apparent self-inflicted gunshot wound.

20 23. Officers found multiple firearms and hundreds of rounds of ammunition in the room
21 in close proximity to Paddock's body. Additionally, investigators located over a thousand rounds of
22 ammunition and explosive material in a vehicle associated with Paddock. Further, multiple firearms
23 and a large quantity of ammunition were located at Paddock's residence at 1372 Babbling Brook
24 Court, Mesquite.

1 24. Paddock's Nevada driver's license was located in the Mandalay Bay hotel room with
2 Paddock, and both hotel rooms were registered in his name. A player's club card in name of Marilou
3 Danley was located in Paddock's room, and the card returned to the same Babbling Brook address in
4 Mesquite.

5 25. While monitoring an identified Facebook accounts of Marilou Danley
6 (facebook.com/marilou.danley) after the shooting, LVMPD investigators noted that the account
7 settings and privacy settings were changed on October 2, 2017, at approximately 0030 hours. At
8 approximately 0246 hours, the Facebook account was deleted. Investigators discovered the
9 following additional Instagram accounts associated with Stephen Paddock and Marilou Paddock:
10 **stephenpaddock47, mariloudanley, mariloudanleyy, mariloudanleypaddock, and**
11 **marilou.danley.** On October 3, 2017, a preservation request for all content pertaining to the these
12 Instagram was submitted to Facebook to maximize the chance that the contents of the account
13 remain preserved.

14 26. Based on my training and experience, a person who possesses large amounts of
15 firearms and ammunition obtains those items over a period of time. Thus, I am requesting that the
16 search period be from September 1, 2016 to the present.

17 27. Based on these stated facts, it is your Affiant's opinion that there is probable cause to
18 believe that the Instagram accounts with user IDs **stephenpaddock47, mariloudanley,**
19 **mariloudanleyy, mariloudanleypaddock, and marilou.danley** contain evidence related to
20 **PADDOCK's** possession of firearms in violation of Title 26, United States Code, Section 5841.
21 Your Affiant also submits that a review of photos and other non-public content on the subject
22 accounts will likely produce further evidence of prior and additional violations of the enumerated
23 offenses. I swear, under penalty of perjury, that the foregoing is true and correct to the best of my
24 knowledge and belief.

1 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

2 28. Your Affiant anticipates executing this warrant under the Electronic Communications
3 Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the
4 warrant to require Facebook to disclose to the government copies of the records and other
5 information (including the content of communications) particularly described in Section I of
6 Attachment "B." Upon receipt of the information described in Section I of Attachment "B,"
7 government-authorized persons will review that information to locate the items described in Section
8 II of Attachment "B."

9 **CONCLUSION**

10 29. Based on the information set forth herein, Your Affiant has probable cause to believe
11 that in the subject accounts listed in Attachments "A1", "A2", "A3", "A4", "A5" there is proof that
12 constitutes evidence of the commission of criminal offense(s); contraband, the fruits of crime and
13 things otherwise criminally possessed; and property designed or intended for use or which is or has
14 been used as the means of committing criminal offense(s). The evidence to be searched for and
15 seized is set forth in Attachment "B", which is attached hereto and incorporated herein by reference.

16 30. Based on the forgoing, your Affiant requests that the Court issue the proposed search
17 warrant.

18 31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not
19 required for the service or execution of this warrant.

20 **REQUEST FOR SEALING**

21 31. I further request that the Court order that all papers in support of this application,
22 including the affidavit and search warrant, be sealed until further order of the Court. These
23 documents discuss an ongoing criminal investigation that is neither public nor known to all of the
24

1 targets of the investigation. Accordingly, there is good cause to seal these documents because their
2 premature disclosure may seriously jeopardize that investigation.

3
4 Respectfully Submitted,

5
6 1/51
Heather D. Burton, Special Agent
7 Federal Bureau of Investigation

8 SWORN TO AND SUBSCRIBED
9 before me this 3rd day of October, 2017.

10 CAM FERENBACH
11 UNITED STATES MAGISTRATE JUDGE

12
13
14 I hereby attest and certify on 10-3-17
15 that the foregoing document is a full true and correct
16 copy of the original on file in my office, and in my legal
17 custody.

18 CAM FERENBACH
19 U.S. MAGISTRATE JUDGE
20 DISTRICT OF NEVADA

21 By Meln Deputy
22 Secretary

Attachment "A1"

Property to Be Searched

This warrant applies to information associated with the Instagram user IDs **stephenpaddock47**, that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California for the time period beginning September 1, 2016 to present.

Attachment "A2"

Property to Be Searched

This warrant applies to information associated with the Instagram user IDs **mariloudanley**, that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California for the time period beginning September 1, 2016 to present.

Attachment "A3"

Property to Be Searched

This warrant applies to information associated with the Instagram user IDs **mariloudanleey**, that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California for the time period beginning September 1, 2016 to present.

Attachment "A4"

Property to Be Searched

This warrant applies to information associated with the Instagram user IDs **mariloudanleypaddock**, that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California for the time period beginning September 1, 2016 to present.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

1 ATTACHMENT "B"

2 Particular Things to be Seized

3 I. Information to be disclosed by Facebook

4 To the extent that the information described in Attachment A is within the possession,
5 custody, or control of Instagram LLC ("Instagram"), including any messages, records, files, logs, or
6 information that have been deleted but are still available to Instagram, or have been preserved pursuant
7 to a request made under 18 U.S.C. § 2703(f) on October 3, 2017. Facebook is required to disclose the
8 following information to the government for each user IDs listed in Attachment A for the period of
9 September 1, 2016 to present:

- 10 (a) All contact and personal identifying information, including: full name, user
11 identification number, birth date, gender, contact e-mail addresses, Instagram
12 passwords, Instagram security questions and answers, physical address (including
13 city, state, and zip code), telephone numbers, screen names, websites, and other
14 personal identifiers;
- 15 (b) All activity logs for the account and all other documents showing the user's posts and
16 other Instagram activities;
- 17 (c) All photos and videos uploaded by that user ID and all photos and videos uploaded
18 by any user that have that user tagged in them;
- 19 (d) All profile information; status updates; links to videos, photographs, bios, articles,
20 and other items; Wall postings; friend lists, including the friends' Instagram user
21 identification numbers; future and past event postings; comments; and tags;
- 22 (e) All other records of communications and messages made or received by the user, chat
23 history, and pending "Friend" requests;
24

- (f) All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content;
- (g) All IP logs, including all records of the IP addresses that logged into the account;
- (h) All records of the account's usage of the "Like" feature, including all Instagram posts and content that the user has "liked";
- (i) All location data associated with the account, including geotags;
- (j) All data and information that has been deleted by the user;
- (k) All past and present lists of friends created by the account;
- (l) All records of Instagram searches performed by the account;
- (m) The types of service utilized by the user;
- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (o) All privacy settings and other account settings, including privacy settings for individual Instagram posts and activities, and all records showing which Instagram users have been blocked by the account;
- (p) All records pertaining to communications between Instagram and any person regarding the user or the user's Instagram account, including contacts with support services and records of actions taken.
- (q) All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;

1 **II. Information to be seized by the government**

2 All information described above in Section I that constitutes fruits, evidence, and instrumentalities
3 of violations of:

4 Violation of National Firearms Act – Registration of Firearms, Title 26, United States Code,
5 Section 5841.

6 involving STEPHEN PADDOCK and others yet unidentified, including, for each user ID identified
7 on Attachment "A," information pertaining to the following matters:

- 8 (a) Evidence showing the possession, use, purchase, or sale of firearms, firearms
9 accessories, ammunition, or explosives by Paddock, including through conspiring and
10 cooperating to possess, use, purchase, or sell prohibited firearms, firearms
11 accessories, ammunition, or explosives.
- 12 (b) Evidence indicating how and when the Instagram account was accessed or used, to
13 determine the chronological and geographic context of account access, use, and
14 events relating to the crime under investigation and to the Facebook account owner;
- 15 (c) Evidence indicating the Instagram account owner's state of mind as it relates to the
16 crime under investigation;
- 17 (d) The identity of the person(s) who created or used the user ID, including records that
18 help reveal the whereabouts of such person(s).
- 19 (e) The identity of the person(s) who communicated with the user ID about matters
20 relating to the illegal possession, purchase, use, or sale of firearms, firearms
21 accessories, ammunition, or explosives, including records that help reveal their
22 whereabouts.

23 **The Warrant expressly incorporates the Affidavit submitted in support of the Warrant, and**
24 **separately sealed, as though set forth fully herein.**

1 ATTACHMENT C

2 PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED

3 PURSUANT TO THIS SEARCH WARRANT

4 1. In executing this warrant, the government must make reasonable efforts to use
5 methods and procedures that will locate and expose in the electronic data produced in response to
6 this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other
7 electronically stored information that are identified with particularity in the warrant, while
8 minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent
9 reasonably practicable.

10 2. When the Search Warrant Data is received, the government will make a duplicate
11 copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the
12 Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to
13 return or dispose of the Search Warrant Data; production to the defense in any criminal case if
14 authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the
15 Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The
16 original of the Search Warrant Data will not be searched or examined except to ensure that it has
17 been fully and completely replicated in the Search Warrant Data Copy.

18 3. The investigating agents will then search the entirety of the Search Warrant Data
19 Copy using any and all methods and procedures deemed appropriate by the United States designed
20 to identify the information listed as Information to be Seized in Attachment B, Section II. The
21 United States may copy, extract or otherwise segregate information or data listed as Information to
22 be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise
23 segregated will no longer be subject to any handling restrictions that might be set out in this protocol
24 beyond those required by binding law. To the extent evidence of crimes not within the scope of this
warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be
applied for in order to further search that document, data, or other item.

4. The Government will have ninety (90) days from receipt of the data disclosed under
Attachment B, Section I to complete its examination of the Search Warrant Data Copy. Once the
Search Warrant Data Copy has been thoroughly and completely examined for any document, data,
or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant
Data Copy will be sealed and not subject to any further search or examination unless authorized by
another search warrant or other appropriate court order. The Search Warrant Data Copy will be held
and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the
investigating and prosecuting authorities, and may include the following techniques (the following is
a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
- f. scanning storage areas;
- g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and

1 (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later
2 off-site copying or review.

3 (f) Executing and Returning the Warrant.

4 (1) Warrant to Search for and Seize a Person or Property.

5 (B) Inventory. An officer present during the execution of the warrant must prepare and verify
6 an inventory of any property seized. . . . In a case involving the seizure of electronic storage media
7 or the seizure or copying of electronically stored information, the inventory may be limited to
8 describing the physical storage media that were seized or copied. The officer may retain a copy of
9 the electronically stored information that was seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in accordance with the
11 following:

12 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the
13 warrant, an agent is required to file an inventory return with the Court, that is, to file an
14 itemized list of the property seized. Execution of the warrant begins when the United States
15 serves the warrant on the named custodian; execution is complete when the custodian
16 provides all Search Warrant Data to the United States. Within fourteen (14) days of
17 completion of the execution of the warrant, the inventory will be filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the
19 electronically stored information must be seized after the issuance of the warrant and copied
20 after the execution of the warrant, not the "later review of the media or information" seized,
21 or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be
23 limited to a description of the "physical storage media" into which the Search Warrant Data
24 that was seized was placed, not an itemization of the information or data stored on the
"physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes
of the investigation. The government proposes that the original storage media on which the
Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be
retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any
information in the Search Warrant Data that is not set forth in Attachment B, Section II, that
information will be copied onto appropriate media and returned to the person from whom the
information was seized.

10-3-17

UNITED STATES DISTRICT COURT

for the
District of NevadaI hereby attest and certify on _____
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADAIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INSTAGRAM ACCOUNTS STORED AT
PREMISES CONTROLLED BY
FACEBOOK CORPORATION: stephenpaddock47 A1By [Signature]
Case No. 2:17-mj-00958-VCF Deputy Secretary

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION:
stephenpaddock47 A1located in the DEA District of _____, there is now concealed (identify the
person or describe the property to be seized):INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION:
stephenpaddock47 A1

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 26, United States Code, Section 5841.	Violation of National Firearms Act

The application is based on these facts:
I believe there is probable cause to believe that in the subject accounts listed in Attachments "A1", "A2", "A3",
"A4", "A5" there is proof that constitutes evidence of the commission of criminal offense(s); contraband, the fruits
of crime and things otherwise criminally possessed and been used as the means of committing criminal offense(s)☐ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Printed name and title

Sworn to before me and signed in my presence.

CAM FERENBACH

Date:

10-3-17

Las Vegas, Nevada

City and state:

Judge's signature

CAM FERENBACH

U.S. MAGISTRATE JUDGE
Printed name and titleFILED
2017 OCT -3 PM 3:34
U.S. MAGISTRATE JUDGE
BY _____

I hereby attest and certify on 10-3-17
 that the foregoing document is a full true and correct
 copy of the original on file in my office, and in my legal
 custody.

UNITED STATES DISTRICT COURT

for the
 District of Nevada

CAM FERENBACH
 U.S. MAGISTRATE JUDGE
 DISTRICT OF NEVADA

By Mota

☒ Deputy
 Secretary

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)

stephenpaddock47 A1

Case No. 2:17-mj-00958-VCF

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
 of the following person or property located in the _____ District of _____ Nevada
 (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
 described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

YOU ARE COMMANDED to execute this warrant on or before 10-12-17 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
 person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
 property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
 as required by law and promptly return this warrant and inventory to CAM FERENBACH

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
 § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
 property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 10-3-17 4:03pm

CAM FERENBACH

Judge's signature

City and state: Las Vegas, Nevada

CAM FERENBACH
 U.S. MAGISTRATE JUDGE
 Printed name and title



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

Attachment "A1"

Property to Be Searched

This warrant applies to information associated with the Instagram user IDs **stephenpaddock47**, that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California for the time period beginning September 1, 2016 to present.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "B"

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Instagram LLC ("Instagram"), including any messages, records, files, logs, or information that have been deleted but are still available to Instagram, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 3, 2017. Facebook is required to disclose the following information to the government for each user IDs listed in Attachment A for the period of September 1, 2016 to present:

- (a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, Instagram passwords, Instagram security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All activity logs for the account and all other documents showing the user's posts and other Instagram activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (d) All profile information; status updates; links to videos, photographs, bios, articles, and other items; Wall postings; friend lists, including the friends' Instagram user identification numbers; future and past event postings; comments; and tags;
- (e) All other records of communications and messages made or received by the user, chat history, and pending "Friend" requests;

- 1 (f) All user content created, uploaded, or shared by the account, including any comments
2 made by the account on photographs or other content;
- 3 (g) All IP logs, including all records of the IP addresses that logged into the account;
- 4 (h) All records of the account's usage of the "Like" feature, including all Instagram posts
5 and content that the user has "liked";
- 6 (i) All location data associated with the account, including geotags;
- 7 (j) All data and information that has been deleted by the user;
- 8 (k) All past and present lists of friends created by the account;
- 9 (l) All records of Instagram searches performed by the account;
- 10 (m) The types of service utilized by the user;
- 11 (n) The length of service (including start date) and the means and source of any payments
12 associated with the service (including any credit card or bank account number);
- 13 (o) All privacy settings and other account settings, including privacy settings for
14 individual Instagram posts and activities, and all records showing which Instagram
15 users have been blocked by the account;
- 16 (p) All records pertaining to communications between Instagram and any person
17 regarding the user or the user's Instagram account, including contacts with support
18 services and records of actions taken.
- 19 (q) All information regarding the particular device or devices used to login to or access
20 the account, including all device identifier information or cookie information,
21 including all information about the particular device or devices used to access the
22 account and the date and time of those accesses;
- 23
24

1 **II. Information to be seized by the government**

2 All information described above in Section I that constitutes fruits, evidence, and instrumentalities
3 of violations of:

4 Violation of National Firearms Act – Registration of Firearms, Title 26, United States Code,
5 Section 5841.

6 involving STEPHEN PADDOCK and others yet unidentified, including, for each user ID identified
7 on Attachment "A," information pertaining to the following matters:

- 8 (a) Evidence showing the possession, use, purchase, or sale of firearms, firearms
9 accessories, ammunition, or explosives by Paddock, including through conspiring and
10 cooperating to possess, use, purchase, or sell prohibited firearms, firearms
11 accessories, ammunition, or explosives.
- 12 (b) Evidence indicating how and when the Instagram account was accessed or used, to
13 determine the chronological and geographic context of account access, use, and
14 events relating to the crime under investigation and to the Facebook account owner;
- 15 (c) Evidence indicating the Instagram account owner's state of mind as it relates to the
16 crime under investigation;
- 17 (d) The identity of the person(s) who created or used the user ID, including records that
18 help reveal the whereabouts of such person(s).
- 19 (e) The identity of the person(s) who communicated with the user ID about matters
20 relating to the illegal possession, purchase, use, or sale of firearms, firearms
21 accessories, ammunition, or explosives, including records that help reveal their
22 whereabouts.

23 **The Warrant expressly incorporates the Affidavit submitted in support of the Warrant, and**
24 **separately sealed, as though set forth fully herein.**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT C

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED

PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. The Government will have ninety (90) days from receipt of the data disclosed under Attachment B, Section I to complete its examination of the Search Warrant Data Copy. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
- f. scanning storage areas;
- g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and

1 (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later
2 off-site copying or review.

3 (f) Executing and Returning the Warrant.

4 (1) Warrant to Search for and Seize a Person or Property.

5 (B) Inventory. An officer present during the execution of the warrant must prepare and verify
6 an inventory of any property seized. . . . In a case involving the seizure of electronic storage media
7 or the seizure or copying of electronically stored information, the inventory may be limited to
8 describing the physical storage media that were seized or copied. The officer may retain a copy of
9 the electronically stored information that was seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in accordance with the
11 following:

12 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the
13 warrant, an agent is required to file an inventory return with the Court, that is, to file an
14 itemized list of the property seized. Execution of the warrant begins when the United States
15 serves the warrant on the named custodian; execution is complete when the custodian
16 provides all Search Warrant Data to the United States. Within fourteen (14) days of
17 completion of the execution of the warrant, the inventory will be filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the
19 electronically stored information must be seized after the issuance of the warrant and copied
20 after the execution of the warrant, not the "later review of the media or information" seized,
21 or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be
23 limited to a description of the "physical storage media" into which the Search Warrant Data
24 that was seized was placed, not an itemization of the information or data stored on the
"physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes
of the investigation. The government proposes that the original storage media on which the
Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be
retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any
information in the Search Warrant Data that is not set forth in Attachment B, Section II, that
information will be copied onto appropriate media and returned to the person from whom the
information was seized.

UNITED STATES DISTRICT COURT

for the
District of NevadaI hereby attest and certify on 10-3-17
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADAIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INSTAGRAM ACCOUNTS STORED AT
PREMISES CONTROLLED BY
FACEBOOK CORPORATION: Mariloudanley A2Case No. By 2:17-mj-00959-VCF A Deputy
Secretary

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):
INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION: Mariloudanley
A2located in the DEA District of , there is now concealed (identify the
person or describe the property to be seized):INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION: Mariloudanley
A2

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 26, United States Code, Section 5841.	Violation of National Firearms Act

The application is based on these facts:
 I believe there is probable cause to believe that in the subject accounts listed in Attachments "A1", "A2", "A3",
 "A4", "A5" there is proof that constitutes evidence of the commission of criminal offense(s); contraband, the fruits
 of crime and things otherwise criminally possessed and been used as the means of committing criminal offense(s)

☐ Continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested
 under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

Printed name and title

Sworn to before me and signed in my presence.

Date: 10-3-17City and state: Las Vegas, Nevada

CAM FERENBACH

CAM FERENBACH
 U.S. MAGISTRATE JUDGE
 Printed name and title

FILED
 2017 OCT -3 PM 3:36
 U.S. MAGISTRATE JUDGE
 BY

UNITED STATES DISTRICT COURT

for the
District of NevadaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Mariloudanley A2

I hereby attest and certify on
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADABy [Signature] Deputy
Secretary

Case No. 2:17-mj-00959-VCF

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

YOU ARE COMMANDED to execute this warrant on or before 10-12-17 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to CAM FERENBACH
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

10-3-17 4:04p

CAM FERENBACH

[Signature]
CAM FERENBACH

U.S. MAGISTRATE JUDGE

Printed name and title

City and state:

Las Vegas, Nevada



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

Attachment "A2"

Property to Be Searched

This warrant applies to information associated with the Instagram user IDs **mariloudanley**, that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California for the time period beginning September 1, 2016 to present.

1

2

3

4

- 10

- 1 (f) All user content created, uploaded, or shared by the account, including any comments
2 made by the account on photographs or other content;
- 3 (g) All IP logs, including all records of the IP addresses that logged into the account;
- 4 (h) All records of the account's usage of the "Like" feature, including all Instagram posts
5 and content that the user has "liked";
- 6 (i) All location data associated with the account, including geotags;
- 7 (j) All data and information that has been deleted by the user;
- 8 (k) All past and present lists of friends created by the account;
- 9 (l) All records of Instagram searches performed by the account;
- 10 (m) The types of service utilized by the user;
- 11 (n) The length of service (including start date) and the means and source of any payments
12 associated with the service (including any credit card or bank account number);
- 13 (o) All privacy settings and other account settings, including privacy settings for
14 individual Instagram posts and activities, and all records showing which Instagram
15 users have been blocked by the account;
- 16 (p) All records pertaining to communications between Instagram and any person
17 regarding the user or the user's Instagram account, including contacts with support
18 services and records of actions taken.
- 19 (q) All information regarding the particular device or devices used to login to or access
20 the account, including all device identifier information or cookie information,
21 including all information about the particular device or devices used to access the
22 account and the date and time of those accesses;
- 23
24

1 **II. Information to be seized by the government**

2 All information described above in Section I that constitutes fruits, evidence, and instrumentalities
3 of violations of:

4 Violation of National Firearms Act – Registration of Firearms, Title 26, United States Code,
5 Section 5841.

6 involving STEPHEN PADDOCK and others yet unidentified, including, for each user ID identified
7 on Attachment “A,” information pertaining to the following matters:

8 (a) Evidence showing the possession, use, purchase, or sale of firearms, firearms
9 accessories, ammunition, or explosives by Paddock, including through conspiring and
10 cooperating to possess, use, purchase, or sell prohibited firearms, firearms
11 accessories, ammunition, or explosives.

12 (b) Evidence indicating how and when the Instagram account was accessed or used, to
13 determine the chronological and geographic context of account access, use, and
14 events relating to the crime under investigation and to the Facebook account owner;

15 (c) Evidence indicating the Instagram account owner’s state of mind as it relates to the
16 crime under investigation;

17 (d) The identity of the person(s) who created or used the user ID, including records that
18 help reveal the whereabouts of such person(s).

19 (e) The identity of the person(s) who communicated with the user ID about matters
20 relating to the illegal possession, purchase, use, or sale of firearms, firearms
21 accessories, ammunition, or explosives, including records that help reveal their
22 whereabouts.

23 **The Warrant expressly incorporates the Affidavit submitted in support of the Warrant, and**
24 **separately sealed, as though set forth fully herein.**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT C

**PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT**

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. The Government will have ninety (90) days from receipt of the data disclosed under Attachment B, Section I to complete its examination of the Search Warrant Data Copy. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
- f. scanning storage areas;
- g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and

1 (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later
2 off-site copying or review.

3 (f) Executing and Returning the Warrant.

4 (1) Warrant to Search for and Seize a Person or Property.

5 (B) Inventory. An officer present during the execution of the warrant must prepare and verify
6 an inventory of any property seized. . . . In a case involving the seizure of electronic storage media
7 or the seizure or copying of electronically stored information, the inventory may be limited to
8 describing the physical storage media that were seized or copied. The officer may retain a copy of
9 the electronically stored information that was seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in accordance with the
11 following:

12 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the
13 warrant, an agent is required to file an inventory return with the Court, that is, to file an
14 itemized list of the property seized. Execution of the warrant begins when the United States
15 serves the warrant on the named custodian; execution is complete when the custodian
16 provides all Search Warrant Data to the United States. Within fourteen (14) days of
17 completion of the execution of the warrant, the inventory will be filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the
19 electronically stored information must be seized after the issuance of the warrant and copied
20 after the execution of the warrant, not the "later review of the media or information" seized,
21 or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be
23 limited to a description of the "physical storage media" into which the Search Warrant Data
24 that was seized was placed, not an itemization of the information or data stored on the
"physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes
of the investigation. The government proposes that the original storage media on which the
Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be
retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any
information in the Search Warrant Data that is not set forth in Attachment B, Section II, that
information will be copied onto appropriate media and returned to the person from whom the
information was seized.

UNITED STATES DISTRICT COURT

for the
District of NevadaI hereby attest and certify on 10-3-17
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
INSTAGRAM ACCOUNTS STORED AT
PREMISES CONTROLLED BY
FACEBOOK CORPORATION: Mariloudanleyy A3

Case No. 2:17-mj-00960-VCF

By [Signature] Deputy
SecretaryCAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION:
Mariloudanleyy A3located in the DEA District of _____, there is now concealed (identify the
person or describe the property to be seized):INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION: Mariloudanleyy
A3

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 26, United States Code, Section 5841.	Violation of National Firearms Act

The application is based on these facts:
I believe there is probable cause to believe that in the subject accounts listed in Attachments "A1", "A2", "A3",
"A4", "A5" there is proof that constitutes evidence of the commission of criminal offense(s); contraband, the fruits
of crime and things otherwise criminally possessed and been used as the means of committing criminal offense(s)

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

1/51
Applicant's signature

Printed name and title

Sworn to before me and signed in my presence.

Date: 10-3-17City and state Las Vegas, Nevada

CAM FERENBACH

[Signature]
CAM FERENBACH
U.S. MAGISTRATE JUDGE
Printed name and title

10-3-17

UNITED STATES DISTRICT COURT

for the
District of NevadaI hereby attest and certify on _____
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADAIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Mariloudanleyy A3

By *M. Fer* Deputy
Secretary

Case No. 2:17-mj-00960-VCF

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A3

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

YOU ARE COMMANDED to execute this warrant on or before 10-12-17 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to CAM FERENBACH
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

10-3-17 4:04pm

CAM FERENBACH

CAM FERENBACH
Judge's Signature

U.S. MAGISTRATE JUDGE

City and state:

Las Vegas, Nevada

Printed name and title



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "B"

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Instagram LLC ("Instagram"), including any messages, records, files, logs, or information that have been deleted but are still available to Instagram, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 3, 2017. Facebook is required to disclose the following information to the government for each user IDs listed in Attachment A for the period of September 1, 2016 to present:

- (a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, Instagram passwords, Instagram security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All activity logs for the account and all other documents showing the user's posts and other Instagram activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (d) All profile information; status updates; links to videos, photographs, bios, articles, and other items; Wall postings; friend lists, including the friends' Instagram user identification numbers; future and past event postings; comments; and tags;
- (e) All other records of communications and messages made or received by the user, chat history, and pending "Friend" requests;

- (f) All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content;
- (g) All IP logs, including all records of the IP addresses that logged into the account;
- (h) All records of the account's usage of the "Like" feature, including all Instagram posts and content that the user has "liked";
- (i) All location data associated with the account, including geotags;
- (j) All data and information that has been deleted by the user;
- (k) All past and present lists of friends created by the account;
- (l) All records of Instagram searches performed by the account;
- (m) The types of service utilized by the user;
- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (o) All privacy settings and other account settings, including privacy settings for individual Instagram posts and activities, and all records showing which Instagram users have been blocked by the account;
- (p) All records pertaining to communications between Instagram and any person regarding the user or the user's Instagram account, including contacts with support services and records of actions taken.
- (q) All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;

1 **II. Information to be seized by the government**

2 All information described above in Section I that constitutes fruits, evidence, and instrumentalities
3 of violations of:

4 Violation of National Firearms Act – Registration of Firearms, Title 26, United States Code,
5 Section 5841.

6 involving STEPHEN PADDOCK and others yet unidentified, including, for each user ID identified
7 on Attachment "A," information pertaining to the following matters:

- 8 (a) Evidence showing the possession, use, purchase, or sale of firearms, firearms
9 accessories, ammunition, or explosives by Paddock, including through conspiring and
10 cooperating to possess, use, purchase, or sell prohibited firearms, firearms
11 accessories, ammunition, or explosives.
- 12 (b) Evidence indicating how and when the Instagram account was accessed or used, to
13 determine the chronological and geographic context of account access, use, and
14 events relating to the crime under investigation and to the Facebook account owner;
- 15 (c) Evidence indicating the Instagram account owner's state of mind as it relates to the
16 crime under investigation;
- 17 (d) The identity of the person(s) who created or used the user ID, including records that
18 help reveal the whereabouts of such person(s).
- 19 (e) The identity of the person(s) who communicated with the user ID about matters
20 relating to the illegal possession, purchase, use, or sale of firearms, firearms
21 accessories, ammunition, or explosives, including records that help reveal their
22 whereabouts.

23 **The Warrant expressly incorporates the Affidavit submitted in support of the Warrant, and**
24 **separately sealed, as though set forth fully herein.**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT C

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED

PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. The Government will have ninety (90) days from receipt of the data disclosed under Attachment B, Section I to complete its examination of the Search Warrant Data Copy. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
- f. scanning storage areas;
- g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and

1 (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later
2 off-site copying or review.

3 (f) Executing and Returning the Warrant.

4 (1) Warrant to Search for and Seize a Person or Property.

5 (B) Inventory. An officer present during the execution of the warrant must prepare and verify
6 an inventory of any property seized. . . . In a case involving the seizure of electronic storage media
7 or the seizure or copying of electronically stored information, the inventory may be limited to
8 describing the physical storage media that were seized or copied. The officer may retain a copy of
9 the electronically stored information that was seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in accordance with the
11 following:

12 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the
13 warrant, an agent is required to file an inventory return with the Court, that is, to file an
14 itemized list of the property seized. Execution of the warrant begins when the United States
15 serves the warrant on the named custodian; execution is complete when the custodian
16 provides all Search Warrant Data to the United States. Within fourteen (14) days of
17 completion of the execution of the warrant, the inventory will be filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the
19 electronically stored information must be seized after the issuance of the warrant and copied
20 after the execution of the warrant, not the "later review of the media or information" seized,
21 or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be
23 limited to a description of the "physical storage media" into which the Search Warrant Data
24 that was seized was placed, not an itemization of the information or data stored on the
"physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes
of the investigation. The government proposes that the original storage media on which the
Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be
retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any
information in the Search Warrant Data that is not set forth in Attachment B, Section II, that
information will be copied onto appropriate media and returned to the person from whom the
information was seized.

UNITED STATES DISTRICT COURT

for the
District of Nevada

I hereby attest and certify on 10-3-17
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

INSTAGRAM ACCOUNTS STORED AT
PREMISES CONTROLLED BY FACEBOOK
CORPORATION: Mariloudanleypaddock A 4

Case No. 2:17-mj-0096
By [Signature] Deputy
Secretary

CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):
INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION:

Mariloudanleypaddock A4

located in the DEA District of , there is now concealed (identify the
person or describe the property to be seized):

INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION:
Mariloudanleypaddock A4

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 26, United States Code, Section 5841.	Violation of National Firearms Act

The application is based on these facts:
I believe there is probable cause to believe that in the subject accounts listed in Attachments "A1", "A2", "A3",
"A4", "A5" there is proof that constitutes evidence of the commission of criminal offense(s); contraband, the fruits
of crime and things otherwise criminally possessed and been used as the means of committing criminal offense(s)

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

FILED
2017 OCT -3 PM 3:55
U.S. MAGISTRATE JUDGE
BY

151
Applicant's signature

Printed name and title

Sworn to before me and signed in my presence.

Date: 10-3-17

City and state: Las Vegas, Nevada

CAM FERENBACH

[Signature]
CAM FERENBACH
U.S. MAGISTRATE JUDGE
Printed name and title

UNITED STATES DISTRICT COURT

for the
District of NevadaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Mariloudanleypaddock A4

)
)
)
)
)
)

Case No.

I hereby attest and certify on 10-3-17
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA

By

2:17-mj-00961-VCFDeputy
Secretary

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A4

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

☒ YOU ARE COMMANDED to execute this warrant on or before 10-12-17 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to _____CAM FERENBACH
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

10-3-174:08pm

CAM FERENBACH

CAM FERENBACH

City and state:

Las Vegas, Nevada

U.S. MAGISTRATE JUDGE

Printed name and title



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

Attachment "A4"

Property to Be Searched

This warrant applies to information associated with the Instagram user IDs **mariloudanleypaddock**, that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California for the time period beginning September 1, 2016 to present.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "B"

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Instagram LLC ("Instagram"), including any messages, records, files, logs, or information that have been deleted but are still available to Instagram, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 3, 2017. Facebook is required to disclose the following information to the government for each user IDs listed in Attachment A for the period of September 1, 2016 to present:

- (a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, Instagram passwords, Instagram security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All activity logs for the account and all other documents showing the user's posts and other Instagram activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (d) All profile information; status updates; links to videos, photographs, bios, articles, and other items; Wall postings; friend lists, including the friends' Instagram user identification numbers; future and past event postings; comments; and tags;
- (e) All other records of communications and messages made or received by the user, chat history, and pending "Friend" requests;

- 1 (f) All user content created, uploaded, or shared by the account, including any comments
2 made by the account on photographs or other content;
- 3 (g) All IP logs, including all records of the IP addresses that logged into the account;
- 4 (h) All records of the account's usage of the "Like" feature, including all Instagram posts
5 and content that the user has "liked";
- 6 (i) All location data associated with the account, including geotags;
- 7 (j) All data and information that has been deleted by the user;
- 8 (k) All past and present lists of friends created by the account;
- 9 (l) All records of Instagram searches performed by the account;
- 10 (m) The types of service utilized by the user;
- 11 (n) The length of service (including start date) and the means and source of any payments
12 associated with the service (including any credit card or bank account number);
- 13 (o) All privacy settings and other account settings, including privacy settings for
14 individual Instagram posts and activities, and all records showing which Instagram
15 users have been blocked by the account;
- 16 (p) All records pertaining to communications between Instagram and any person
17 regarding the user or the user's Instagram account, including contacts with support
18 services and records of actions taken.
- 19 (q) All information regarding the particular device or devices used to login to or access
20 the account, including all device identifier information or cookie information,
21 including all information about the particular device or devices used to access the
22 account and the date and time of those accesses;
- 23
24

1 **II. Information to be seized by the government**

2 All information described above in Section I that constitutes fruits, evidence, and instrumentalities
3 of violations of:

4 Violation of National Firearms Act – Registration of Firearms, Title 26, United States Code,
5 Section 5841.

6 involving STEPHEN PADDOCK and others yet unidentified, including, for each user ID identified
7 on Attachment “A,” information pertaining to the following matters:

- 8 (a) Evidence showing the possession, use, purchase, or sale of firearms, firearms
9 accessories, ammunition, or explosives by Paddock, including through conspiring and
10 cooperating to possess, use, purchase, or sell prohibited firearms, firearms
11 accessories, ammunition, or explosives.
- 12 (b) Evidence indicating how and when the Instagram account was accessed or used, to
13 determine the chronological and geographic context of account access, use, and
14 events relating to the crime under investigation and to the Facebook account owner;
- 15 (c) Evidence indicating the Instagram account owner’s state of mind as it relates to the
16 crime under investigation;
- 17 (d) The identity of the person(s) who created or used the user ID, including records that
18 help reveal the whereabouts of such person(s).
- 19 (e) The identity of the person(s) who communicated with the user ID about matters
20 relating to the illegal possession, purchase, use, or sale of firearms, firearms
21 accessories, ammunition, or explosives, including records that help reveal their
22 whereabouts.

23 **The Warrant expressly incorporates the Affidavit submitted in support of the Warrant, and**
24 **separately sealed, as though set forth fully herein.**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT C

**PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT**

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. The Government will have ninety (90) days from receipt of the data disclosed under Attachment B, Section I to complete its examination of the Search Warrant Data Copy. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
- f. scanning storage areas;
- g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and

1 (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later
2 off-site copying or review.

3 (f) Executing and Returning the Warrant.

4 (1) Warrant to Search for and Seize a Person or Property.

5 (B) Inventory. An officer present during the execution of the warrant must prepare and verify
6 an inventory of any property seized. . . . In a case involving the seizure of electronic storage media
7 or the seizure or copying of electronically stored information, the inventory may be limited to
8 describing the physical storage media that were seized or copied. The officer may retain a copy of
9 the electronically stored information that was seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in accordance with the
11 following:

12 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the
13 warrant, an agent is required to file an inventory return with the Court, that is, to file an
14 itemized list of the property seized. Execution of the warrant begins when the United States
15 serves the warrant on the named custodian; execution is complete when the custodian
16 provides all Search Warrant Data to the United States. Within fourteen (14) days of
17 completion of the execution of the warrant, the inventory will be filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the
19 electronically stored information must be seized after the issuance of the warrant and copied
20 after the execution of the warrant, not the "later review of the media or information" seized,
21 or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be
23 limited to a description of the "physical storage media" into which the Search Warrant Data
24 that was seized was placed, not an itemization of the information or data stored on the
"physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes
of the investigation. The government proposes that the original storage media on which the
Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be
retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any
information in the Search Warrant Data that is not set forth in Attachment B, Section II, that
information will be copied onto appropriate media and returned to the person from whom the
information was seized.

10-3-17

UNITED STATES DISTRICT COURT

for the
District of NevadaI hereby attest and certify on _____
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADABy *[Signature]* Deputy
Secretary

Case No. 2:17-mj-00962-VCF

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
INSTAGRAM ACCOUNTS STORED AT
PREMISES CONTROLLED BY FACEBOOK
CORPORATION: marilou.danley A5

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION: marilou.danley
A5located in the DEA District of _____, there is now concealed (identify the
person or describe the property to be seized):INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION: marilou.danley
A5

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 26, United States Code, Section 5841.	Violation of National Firearms Act

The application is based on these facts:
I believe there is probable cause to believe that in the subject accounts listed in Attachments "A1", "A2", "A3",
"A4", "A5" there is proof that constitutes evidence of the commission of criminal offense(s); contraband, the fruits
of crime and things otherwise criminally possessed and been used as the means of committing criminal offense(s)

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[Signature]
Applicant's signature_____
Printed name and title

Sworn to before me and signed in my presence.

Date: 10-3-17City and state: Las Vegas, Nevada

CAM FERENBACH

[Signature]
CAM FERENBACH
U.S. MAGISTRATE JUDGE_____
Printed name and title

UNITED STATES DISTRICT COURT

for the
District of NevadaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

marilou.danley A5

Case No.

I hereby attest and certify on 10-3-17
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.CAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADABy [Signature]
2:17-mj-00962-VCFDeputy
Secretary

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A5

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

YOU ARE COMMANDED to execute this warrant on or before 10-12-17 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to CAM FERENBACH

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

10-3-17 4:05pm

CAM FERENBACH

Judge's signature

CAM FERENBACH

City and state:

Las Vegas, Nevada

U.S. MAGISTRATE JUDGE

Printed name and title



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

Attachment "A5"

Property to Be Searched

This warrant applies to information associated with the Instagram user IDs and **marilou.danley** that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California for the time period beginning September 1, 2016 to present.

1 ATTACHMENT "B"

2 Particular Things to be Seized

3 I. Information to be disclosed by Facebook

4 To the extent that the information described in Attachment A is within the possession,
5 custody, or control of Instagram LLC ("Instagram"), including any messages, records, files, logs, or
6 information that have been deleted but are still available to Instagram, or have been preserved pursuant
7 to a request made under 18 U.S.C. § 2703(f) on October 3, 2017. Facebook is required to disclose the
8 following information to the government for each user IDs listed in Attachment A for the period of
9 September 1, 2016 to present:

- 10 (a) All contact and personal identifying information, including: full name, user
11 identification number, birth date, gender, contact e-mail addresses, Instagram
12 passwords, Instagram security questions and answers, physical address (including
13 city, state, and zip code), telephone numbers, screen names, websites, and other
14 personal identifiers;
- 15 (b) All activity logs for the account and all other documents showing the user's posts and
16 other Instagram activities;
- 17 (c) All photos and videos uploaded by that user ID and all photos and videos uploaded
18 by any user that have that user tagged in them;
- 19 (d) All profile information; status updates; links to videos, photographs, bios, articles,
20 and other items; Wall postings; friend lists, including the friends' Instagram user
21 identification numbers; future and past event postings; comments; and tags;
- 22 (e) All other records of communications and messages made or received by the user, chat
23 history, and pending "Friend" requests;
24

1 **II. Information to be seized by the government**

2 All information described above in Section I that constitutes fruits, evidence, and instrumentalities
3 of violations of:

4 Violation of National Firearms Act – Registration of Firearms, Title 26, United States Code,
5 Section 5841.

6 involving STEPHEN PADDOCK and others yet unidentified, including, for each user ID identified
7 on Attachment "A," information pertaining to the following matters:

- 8 (a) Evidence showing the possession, use, purchase, or sale of firearms, firearms
9 accessories, ammunition, or explosives by Paddock, including through conspiring and
10 cooperating to possess, use, purchase, or sell prohibited firearms, firearms
11 accessories, ammunition, or explosives.
- 12 (b) Evidence indicating how and when the Instagram account was accessed or used, to
13 determine the chronological and geographic context of account access, use, and
14 events relating to the crime under investigation and to the Facebook account owner;
- 15 (c) Evidence indicating the Instagram account owner's state of mind as it relates to the
16 crime under investigation;
- 17 (d) The identity of the person(s) who created or used the user ID, including records that
18 help reveal the whereabouts of such person(s).
- 19 (e) The identity of the person(s) who communicated with the user ID about matters
20 relating to the illegal possession, purchase, use, or sale of firearms, firearms
21 accessories, ammunition, or explosives, including records that help reveal their
22 whereabouts.

23 **The Warrant expressly incorporates the Affidavit submitted in support of the Warrant, and**
24 **separately sealed, as though set forth fully herein.**

- 1 (f) All user content created, uploaded, or shared by the account, including any comments
- 2 made by the account on photographs or other content;
- 3 (g) All IP logs, including all records of the IP addresses that logged into the account;
- 4 (h) All records of the account's usage of the "Like" feature, including all Instagram posts
- 5 and content that the user has "liked";
- 6 (i) All location data associated with the account, including geotags;
- 7 (j) All data and information that has been deleted by the user;
- 8 (k) All past and present lists of friends created by the account;
- 9 (l) All records of Instagram searches performed by the account;
- 10 (m) The types of service utilized by the user;
- 11 (n) The length of service (including start date) and the means and source of any payments
- 12 associated with the service (including any credit card or bank account number);
- 13 (o) All privacy settings and other account settings, including privacy settings for
- 14 individual Instagram posts and activities, and all records showing which Instagram
- 15 users have been blocked by the account;
- 16 (p) All records pertaining to communications between Instagram and any person
- 17 regarding the user or the user's Instagram account, including contacts with support
- 18 services and records of actions taken.
- 19 (q) All information regarding the particular device or devices used to login to or access
- 20 the account, including all device identifier information or cookie information,
- 21 including all information about the particular device or devices used to access the
- 22 account and the date and time of those accesses;
- 23
- 24

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT C

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED

PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. The Government will have ninety (90) days from receipt of the data disclosed under Attachment B, Section I to complete its examination of the Search Warrant Data Copy. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
- f. scanning storage areas;
- g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and

1 (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later
2 off-site copying or review.

3 (f) Executing and Returning the Warrant.

4 (1) Warrant to Search for and Seize a Person or Property.

5 (B) Inventory. An officer present during the execution of the warrant must prepare and verify
6 an inventory of any property seized. . . . In a case involving the seizure of electronic storage media
7 or the seizure or copying of electronically stored information, the inventory may be limited to
8 describing the physical storage media that were seized or copied. The officer may retain a copy of
9 the electronically stored information that was seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in accordance with the
11 following:

12 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the
13 warrant, an agent is required to file an inventory return with the Court, that is, to file an
14 itemized list of the property seized. Execution of the warrant begins when the United States
15 serves the warrant on the named custodian; execution is complete when the custodian
16 provides all Search Warrant Data to the United States. Within fourteen (14) days of
17 completion of the execution of the warrant, the inventory will be filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the
19 electronically stored information must be seized after the issuance of the warrant and copied
20 after the execution of the warrant, not the "later review of the media or information" seized,
21 or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be
23 limited to a description of the "physical storage media" into which the Search Warrant Data
24 that was seized was placed, not an itemization of the information or data stored on the
"physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes
of the investigation. The government proposes that the original storage media on which the
Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be
retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any
information in the Search Warrant Data that is not set forth in Attachment B, Section II, that
information will be copied onto appropriate media and returned to the person from whom the
information was seized.



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

UNITED STATES DISTRICT COURT

for the
District of Nevada

2017 OCT 13 PM 12:37

U.S. MAGISTRATE JUDGE

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

EMAIL ACCOUNT MARILOUROSES@LIVE.COM THAT
IS STORED AT A PREMISES CONTROLLED BY
MICROSOFT. A2

BY _____
Case No. 2:17-mj-01010-NJK

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

YOU ARE COMMANDED to execute this warrant on or before October 27, 2017 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to NANCY J. KOPPE
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 10/13/17 12:30 p.m.

City and state: Las Vegas, Nevada

NANCY J. KOPPE

Judge's signature

UNITED STATES MAGISTRATE JUDGE

Printed name and title

1 ATTACHMENT "A-2"

2 ONLINE ACCOUNT TO BE SEARCHED

3 This warrant applies to information associated with the Microsoft email account
4 marilouroses@live.com (the "Target Account 2") from inception to present, which is
5 stored at premises owned, maintained, controlled, or operated by Microsoft Corporation,
6 headquartered at 1 Microsoft Way, Redmond, Washington, 98052.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachments A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachments A-1 and A-2 from account inception to present:

- a. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any OneDrive accounts associated with or assigned to Target Accounts 1 and 2.
- b. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Office 360 accounts associated with or assigned to Target Accounts 1 and 2.
- c. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Microsoft Family Safety accounts or services associated with or assigned to Target Accounts 1 and 2.
- d. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Writer accounts or services associated with or assigned to Target Accounts 1 and 2.
- e. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Mail accounts or services associated with or assigned to Target Accounts 1 and 2.
- f. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Photo Gallery accounts or services associated with or assigned to Target Accounts 1 and 2.
- g. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Messenger accounts or services associated with or assigned to Target Accounts 1 and 2.

1 II. Information to be seized by the United States

2 After reviewing all information described in Section I, the United States will seize
3 evidence of violations of Title 18, United States Code Sections 32(a)
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
5 International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of
Firearms by Non Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject
Offenses") that occur in the form of the following, from account inception to present:

- 6 a. Communications, transactions and records that may establish ownership
7 and control (or the degree thereof) of the Target Account, including address
8 books, contact or buddy lists, bills, invoices, receipts, registration records,
9 bills, correspondence, notes, records, memoranda, telephone/address books,
10 photographs, video recordings, audio recordings, lists of names, records of
11 payment for access to newsgroups or other online subscription services, and
12 attachments to said communications, transactions and records.
- 13 b. Communications, transactions and records to/from persons who may be co-
14 conspirators of the Subject Offenses, or which may identify co-conspirators.
- 15 c. Communications, transactions and records which may show motivation to
16 commit the Subject Offenses.
- 17 d. Communications, transactions and records that relate to the Subject
18 Offenses.
- 19 e. The terms "communications," "transactions," "records," "documents,"
20 "programs," or "materials" include all information recorded in any form,
21 visual or aural, and by any means, whether in handmade form (including,
22 but not limited to, writings, drawings, paintings), photographic form
23 (including, but not limited to, pictures or videos), or electrical, electronic or
24 magnetic form, as well as digital data files. These terms also include any
applications (i.e. software programs). These terms expressly include, among
other things, Emails, instant messages, chat logs, correspondence attached
as to Emails (or drafts), calendar entries, buddy lists.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "C"

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

1 5. The search procedures utilized for this review are at the sole discretion of
2 the investigating and prosecuting authorities, and may include the following techniques
(the following is a non-exclusive list, as other search procedures may be used):

3 a. examination of all of the data contained in the Search Warrant Data to view
4 the data and determine whether that data falls within the items to be seized as set forth
herein;

5 b. searching for and attempting to recover from the Search Warrant Data any
6 deleted, hidden, or encrypted data to determine whether that data falls within the list
7 of items to be seized as set forth herein (any data that is encrypted and unreadable will
8 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

9 c. surveying various file directories and the individual files they contain;

10 d. opening files in order to determine their contents;

11 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

12 f. scanning storage areas;

13 g. performing keyword searches through all electronic storage areas to
14 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A1 and A2; and/or

15 h. performing any other data analysis technique that may be necessary to
16 locate and retrieve the evidence described in Attachment B, Section II.

17 Return and Review Procedures

18 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

19 (e) Issuing the Warrant.

20 (2) Contents of the Warrant.

21 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
22 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
23 be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
4 copying of electronically stored information. Unless otherwise specified, the warrant
5 authorizes a later review of the media or information consistent with the warrant. The
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
7 on-site copying of the media or information, and not to any later off-site copying or
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare
9 and verify an inventory of any property seized. . . . In a case involving the seizure of
10 electronic storage media or the seizure or copying of electronically stored information,
11 the inventory may be limited to describing the physical storage media that were seized
12 or copied. The officer may retain a copy of the electronically stored information that was
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
15 of the warrant, an agent is required to file an inventory return with the Court, that is,
16 to file an itemized list of the property seized. Execution of the warrant begins when
17 the United States serves the warrant on the named custodian; execution is complete
18 when the custodian provides all Search Warrant Data to the United States. Within
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be
20 filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
19 which the electronically stored information must be seized after the issuance of the
20 warrant and copied after the execution of the warrant, not the "later review of the media
21 or information" seized, or the later off-site digital copying of that media.

20 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
21 may be limited to a description of the "physical storage media" into which the Search
22 Warrant Data that was seized was placed, not an itemization of the information or data
23 stored on the "physical storage media" into which the Search Warrant Data was placed;
24

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
2 purposes of the investigation. The government proposes that the original storage media
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return
5 of any information in the Search Warrant Data that is not set forth in Attachment B,
6 Section II, that information will be copied onto appropriate media and returned to the
7 person from whom the information was seized.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



FILED

2017 OCT 13 PM 12:36

U.S. MAGISTRATE JUDGE

BY _____

SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

FILED

2017 OCT 13 PM 12:36

U.S. MAGISTRATE JUDGE

BY _____

STEVEN W. MYHRE
Acting United States Attorney
District of Nevada
CRISTINA D. SILVA
PATRICK BURNS
Assistant United States Attorneys
501 Las Vegas Blvd. South, Ste. 1100
Las Vegas, Nevada 89101
Telephone: (702) 388-6336
Fax (702) 388-6698
john.p.burns@usdoj.gov

Attorney for the United States of America

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

-oOo-

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
EMAIL ACCOUNT
CENTRALPARK1@LIVE.COM THAT IS
STORED AT A PREMISES
CONTROLLED BY MICROSOFT.

A1

Magistrate No.

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH
WARRANTS

(Under Seal)

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
EMAIL ACCOUNT
MARILOUROSES@LIVE.COM THAT IS
STORED AT A PREMISES
CONTROLLED BY MICROSOFT.

A2

Magistrate No. 2:17-mj-01010-NJK

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH
WARRANTS

(Under Seal)

STATE OF NEVADA)
) ss:
COUNTY OF CLARK)

///

///

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR SEARCH WARRANTS**

I, Zachary C. McKinney, Special Agent, Federal Bureau of Investigation (FBI),
having been duly sworn, hereby depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant makes this affidavit in support of an application for search warrants for information associated with email accounts centralpark1@live.com ("Target Account 1") and marilouroses@live.com ("Target Account 2"). Target Account 1 is an account associated with STEPHEN PADDOCK. Target Account 2 is an account associated with MARILOU DANLEY. The information associated with both accounts is stored at a premises owned, maintained, controlled, or operated by Microsoft Corporation ("Microsoft"), an American multinational technology company based in Redmond, Washington that specializes in Internet-related services and products along with the development and manufacturing of computer-related items. Those online services include, but are not limited to, email services, cloud computing, and many other services. The information to be searched is described in the following paragraphs and in Attachment "A" (attached hereto and incorporated herein by reference). This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Target Accounts.

2. I am a Special Agent with the Federal Bureau of Investigation, currently assigned to Las Vegas, Nevada. I have been employed as a Special Agent of the FBI since

1 March of 2017. Over the course of my employment with the FBI, I have conducted
2 surveillance, analyzed telephone records, interviewed witnesses, supervised activities of
3 sources, executed search warrants, and executed arrest warrants. These investigative
4 activities have been conducted in conjunction with a variety of investigations, to include
5 those involving robbery, drug trafficking, human trafficking, criminal enterprises, and
6 more. In addition to my practical experiences, I received five months of extensive law
7 enforcement training at the FBI Academy. Previous to the FBI, I was employed as a
8 human intelligence gatherer with the United States Army. I was trained extensively in
9 interrogation, interview, and source handling techniques and best practices. I also
10 received an MBA in International Business and worked with ExxonMobil as a financial
11 manager.

12 3. I make this affidavit in support of an application for a search warrant for
13 information associated with the Microsoft accounts associated with
14 centralpark1@live.com" and "marilouroses@live.com," which is stored at a premises
15 owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at
16 One Microsoft Way, Redmond, WA 98052-6399, hereinafter referred to as "premises,"
17 and further described in Attachments A-1 and A-2 hereto.

- 18 a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C.A. § 32(a);
19 b. Violence at International Airport - 18 U.S.C. § 37(a)(2); and
20 c. Unlawful Interstate Transport/Delivery of Firearms by Non Federal
21 Firearms Licensee - 18 U.S.C. §§ 922(a)(3) and (5);
22 d. Aiding and Abetting - 18 U.S.C. § 2.

1 (hereafter, "Subject Offenses") have been committed by STEPHEN PADDOCK,
2 MARILOU DANLEY, and others yet unknown. There is also probable cause to search
3 the information described in Attachment "A" for evidence of these crimes and
4 information which might reveal the identities of others involved in these crimes, as
5 described in Attachment "B" (attached hereto and incorporated herein by reference).

6 PROBABLE CAUSE

7 4. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music
8 festival, was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At
9 approximately 10:08 p.m., the Las Vegas Metropolitan Police Department (LVMPD)
10 received calls reporting shots had been fired at the concert and multiple victims were
11 struck. LVMPD determined the shots were coming from Rooms 134 and 135 on the 32nd
12 floor of the Mandalay Bay Resort and Casino, located due west of the festival grounds at
13 3950 South Las Vegas Boulevard, Las Vegas, Nevada. These rooms are an elevated
14 position which overlooks the concert venue. Witness statements and video
15 footage captured during the attack indicates that the weapons being used were firing in
16 a fully-automatic fashion.

17 5. LVMPD officers ultimately made entry into the room and located an
18 individual later identified as Stephen Paddock. Paddock was deceased from an apparent
19 self-inflicted gunshot wound.

20 6. Paddock's Nevada driver's license was located in the Mandalay Bay hotel
21 room with Paddock, and both hotel rooms were registered in his name. A player's club
22 card in name of Marilou Danley was located in Paddock's room, and the card returned
23 to the address located on Babbling Brook Street in Mesquite, Nevada. FBI Agents
24

1 located Danley, who was traveling outside the United States at the time of the
2 shooting. It was ultimately determined that Danley resided with Paddock at the
3 Babbling Brook address.

4 7. On October 2, 2017, search warrants were executed on Paddock's Mandalay
5 Bay hotel rooms, Paddock's vehicle at Mandalay Bay, and two Nevada residences owed
6 by Paddock: 1372 Babbling Brook Court in Mesquite, and 1735 Del Webb Parkway in
7 Reno, Nevada. Officers and Agents found over 20 firearms, hundreds of rounds of
8 ammunition, and hundreds of spent shell casings in the Mandalay Bay hotel rooms, in
9 close proximity to Paddock's body. Over a thousand rounds of rifle ammunition and 100
10 pounds of explosive material was found in Paddock's vehicle. Additional explosive
11 material, approximately 18 firearms, and over 1,000 rounds of ammunition was located
12 at the Mesquite residence. A large quantity of ammunition and multiple firearms were
13 recovered from the Reno residence.

14 8. As of this date, 58 people have been identified to have been killed in
15 Paddock's attack and another 557 were reportedly injured. Additionally, investigators
16 discovered that STEPHEN PADDOCK also utilized a firearm to shoot large fuel tanks
17 on Las Vegas McCarran International Airport property. Multiple bullet holes were found
18 on the tank, which investigators believe was an attempt by STEPHEN PADDOCK to
19 cause the tanks to explode.

20 9. In an effort to determine whether or not STEPHEN PADDOCK was
21 assisted and/or conspired with unknown individuals, investigators have attempted to
22 identify all of STEPHEN PADDOCK's associated. It was quickly determined that a
23 casino player's card in the name of MARILOU DANLEY was located in the room at the
24

1 time of the attack. She has been identified thus far as the most likely person who aided
2 or abetted STEPHEN PADDOCK based on her informing law enforcement that her
3 fingerprints would likely be found on the ammunition used during the attack.
4 Subsequently, investigators worked to identify the communication facilities utilized by
5 STEPHEN PADDOCK and MARILOU DANLEY.

6 10. Based on a review of STEPHEN PADDOCK's financial accounts, Target
7 Account 1 was determined to belong to STEPHEN PADDOCK. On October 3, 2017,
8 investigators requested an emergency disclosure of records from Microsoft related to
9 Target Account 1 so it could be immediately searched for any evidence of additional co-
10 conspirators. Unfortunately, the information was only requested for a six-month
11 timeframe. Within the account, investigators identified Target Account 2 as one that
12 belonged to MARILOU DANLEY, which was clear based on the communications
13 between the two email accounts. In an interview, DANLEY stated that PADDOCK had
14 access to one of her email accounts, which investigators believe to be Target Account 2.

15 11. On September 25, 2017, an email was exchanged between the Target
16 Accounts which discussed a wire transfer of funds which was to be sent by STEPHEN
17 PADDOCK to MARILOU DANLEY. It is unclear what the purpose of the wire transfer
18 was, but MARILOU DANLEY is known to have been in the Philippines at the time.

19 12. Additionally, on July 6, 2017, Target Account 1 sent an email to
20 centralpark4804@gmail.com which read, "try an ar before u buy. we have huge selection.
21 located in the las vegas area." Later that day, an email was received back from
22 centralpark4804@gmail.com to Target Account 1 that read, "we have a wide variety of
23 optics and ammunition to try." And lastly, Target Account 1 later sent an email to
24

1 centralpark4804@gmail.com that read, "for a thrill try out bumpfire ar's with a 100
2 round magazine." Investigators believe these communications may have been related to
3 the eventual attack that occurred at the Mandalay Bay in Las Vegas.

4 13. Your Affiant believes the requested search warrants will yield significant
5 information from Microsoft such as STEPHEN PADDOCK's and MARILOU DANLEY's
6 contact lists, email messages content, IP address usage, photographs, third-party
7 applications associated with the account, and more, which may constitute evidence of
8 the planning of the attack and potentially identify other participants in the attack.
9 Ultimately, your Affiant strongly believes the requested information will lead
10 investigators to determine the full scope of STEPHEN PADDOCK's plan and MARILOU
11 DANLEY's possible involvement.

12 14. Investigators have previously sought and obtained a search warrant to
13 examine the contents of both Target Accounts 1 and 2. After execution of that warrant,
14 however, it became apparent and was confirmed with Microsoft that Microsoft was
15 refusing to provide data related to/contained in the OneDrive online storage files for
16 either account. Microsoft indicated to investigators that it did not believe such
17 information was encompassed by the items to be produced that were specified in the
18 original warrant. Investigators believe therefore that there is additional evidence
19 Microsoft currently possesses that relates to the OneDrive online storage service, as well
20 as potentially in a suite of other online services that Microsoft offers, including Office
21 365, Windows Live Mail, Windows Live Writer, Windows Photo Gallery, Windows Live
22 Messenger, Microsoft Family Safety, and Microsoft Outlook Hotmail Connector. Thus,

1 your Affiant seeks more specific authorization to seize and search the OneDrive and
2 other service data specified in Attachment B of the instant warrant application.

3 **RELEVANT TECHNICAL TERMS**

4 15. The following non-exhaustive list of definitions applies to this Affidavit and
5 the Attachments to this Affidavit:

6 a. The "Internet" is a worldwide network of computer systems operated
7 by governmental entities, corporations, and universities. In order to access the Internet,
8 an individual computer user must subscribe to an access provider, which operates a host
9 computer system with direct access to the Internet. The World Wide Web is a
10 functionality of the Internet which allows users of the Internet to share information.

11 b. "Internet Service Providers" are companies that provide access to the
12 Internet. ISPs can also provide other services for their customers including website
13 hosting, email service, remote storage, and co-location of computers and other
14 communications equipment. ISPs offer different ways to access the Internet including
15 telephone-based (dial-up), broadband-based access via a digital subscriber line (DSL) or
16 cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge
17 a fee based upon the type of connection and volume of data (bandwidth). Many ISPs
18 assign each subscriber an account name, such as a user name, an email address, and an
19 email mailbox, and the subscriber typically creates a password for his/her account.

20 c. "ISP Records" are records maintained by ISPs pertaining to their
21 subscribers (regardless of whether those subscribers are individuals or entities). These
22 records may include account application information, subscriber and billing information,
23 account access information (often in the form of log files), emails, information concerning
24

1 content uploaded and/or stored on the ISP's servers, and other information, which may
2 be stored both in computer data format and in written or printed record format. ISPs
3 reserve and/or maintain computer disk storage space on their computer system for their
4 subscribers' use. This service by ISPs allows for both temporary and long-term storage
5 of electronic communications and many other types of electronic data and files.

6 d. "Online service providers" (also referred to here as "service
7 providers") are companies that provide online services such as email, chat or instant
8 messaging, word processing applications, spreadsheet applications, presentation
9 applications similar to PowerPoint, online calendar, photo storage and remote storage
10 services. Sometimes they also can provide web hosting, remote storage, and co-location
11 of computers and other communications equipment. Typically, each service provider
12 assigns each subscriber an account name, such as a user name or screen name and the
13 subscriber typically creates a password for his/her account.

14 e. "Computer," as used herein, is defined as "an electronic, magnetic,
15 optical, electrochemical, or other high speed data processing device performing logical or
16 storage functions, and includes any data storage facility or communications facility
17 directly related to or operating in conjunction with such device."

18 f. A "server" is a centralized computer that provides services for other
19 computers connected to it via a network. The other computers attached to a server are
20 sometimes called "clients." For example, in a large company, it is common for individual
21 employees to have client computers at their desktops. When the employees access their
22 email, or access files stored on the network itself, those files are pulled electronically
23 from the server, where they are stored, and are sent to the client's computer via the
24

1 network. Notably, servers can be physically stored in any location: it is not uncommon
2 for a network's server to be located hundreds (and even thousands) of miles away from
3 the client computers.

4 g. "Internet Protocol address," or "IP address," refers to a unique
5 number used by a computer to access the Internet. IP addresses can be dynamic,
6 meaning that the Internet Service Provider (ISP) assigns a different unique number to
7 a computer every time it accesses the Internet. IP addresses might also be static, that
8 is, an ISP assigns a user's computer a particular IP address which is used each time the
9 computer accesses the Internet.

10 h. The term "domain" refers to a word used as a name for computers,
11 networks, services, etc. A domain name typically represents a website, a server computer
12 that hosts that website, or even some computer (or other digital device) connected to the
13 internet. Essentially, when a website (or a server computer that hosts that website) is
14 connected to the internet, it is assigned an IP address. Because IP addresses are difficult
15 for people to remember, domain names are instead used because they are easier to
16 remember than IP addresses. Domain names are formed by the rules and procedures of
17 the Domain Name System (DNS). A common top level domain under these rules is ".com"
18 for commercial organizations, ".gov" for the United States government, and ".org" for
19 organizations. For example, www.usdoj.gov is the domain name that identifies a server
20 used by the U.S. Department of Justice, and which uses IP address of 149.101.46.71.

21 i. "Web hosting services" maintain server computers connected to the
22 Internet. Their customers use those computers to operate websites on the Internet.
23 Customers of web hosting companies place files, software code, databases, and other data
24

1 on servers. To do this, customers typically connect from their own computers to the
2 server computers across the Internet.

3 j. The term "WhoIs" lookup refers to a search of a publicly available
4 online database that lists information provided when a domain is registered or when an
5 IP address is assigned.

6 k. The terms "communications," "records," "documents," "programs," or
7 "materials" include all information recorded in any form, visual or aural, and by any
8 means, whether in handmade form (including, but not limited to, writings, drawings,
9 paintings), photographic form (including, but not limited to, pictures or videos), or
10 electrical, electronic or magnetic form, as well as digital data files. These terms also
11 include any applications (i.e. software programs). These terms expressly include, among
12 other things, emails, instant messages, chat logs, correspondence attached as to emails
13 (or drafts), calendar entries, buddy lists.

14 l. "Chat" is usually a real time electronic communication between two
15 or more individuals. Unlike email, which is frequently sent, then read and responded to
16 minutes, hours, or even days later, chats frequently involve an immediate conversation
17 between individuals, similar to a face-to-face conversation. Nearly all chat programs are
18 capable of saving the chat transcript, to enable users to preserve a record of the
19 conversation. By default, some chat programs have this capability enabled, while others
20 do not. Many popular web-based email providers, like Microsoft and Microsoft, provide
21 chat functionality as part of the online services they provide to account holders.

22 ///

23 ///

24

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

15
16
17
18
19
20
21
22
23

24

1 18. In general, when a subscriber receives an email, it is typically stored in the
2 subscriber's "mail box" on that service provider's servers until the subscriber deletes the
3 Email. If the subscriber does not delete the message, the message (and any attachments)
4 can remain on that service provider's servers indefinitely.

5 19. Similarly, when the subscriber sends an email, it is initiated at the
6 subscriber's computer, transferred via the Internet to the service provider's servers, and
7 then transmitted to its end destination. That service provider often saves a copy of the
8 email sent. Unless the sender of the email specifically deletes the Email from the
9 provider's server, the email can remain on the system indefinitely.

10 20. A sent or received email typically includes the content of the message,
11 source and destination addresses, the date and time at which the email was sent, and
12 the size and length of the email. If an email user writes a draft message but does not
13 send it, that message may also be saved by that service provider, but may not include all
14 of these categories of data.

15 21. Just as a computer on a desk can be used to store a wide variety of files, so
16 can online accounts, such as the accounts subject to this application. First, subscribers
17 can store many types of files as attachments to emails in online accounts. Second,
18 because service providers provide the services listed above (e.g. word processing,
19 spreadsheets, pictures), subscribers who use these services usually store documents on
20 servers maintained and/or owned by service providers. Thus, these online accounts often
21 contain documents such as pictures, audio or video recordings, logs, spreadsheets,
22 applications and other files.

23
24

1 22. Reviewing files stored in online accounts raises many of the same
2 difficulties as with reviewing files stored on a local computer. For example, based on my
3 training, my experience and this investigation, I know that subscribers of these online
4 services can conceal their activities by altering files before they upload them to the online
5 service. Subscribers can change file names to more innocuous sounding names (e.g.
6 renaming "FraudRecords.doc" to "ChristmasList.doc"), they can change file extensions
7 to make one kind of file appear like a different type of file (e.g. changing the spreadsheet
8 "StolenCreditProfiles.xls" to "FamilyPhoto.jpg" to appear to be a picture file, where the
9 file extension ".xls" denotes an Excel spreadsheet file and ".jpg" a JPEG format image
10 file), or they can change the times and dates a file was last accessed or modified by
11 changing a computer's system time/date and then uploading that file to the Online
12 Accounts. Thus, to detect any files that the subscriber may have concealed, agents will
13 need to review all of the files in the Target Accounts; they will, however, only seize the
14 items that the Court authorizes to be seized. Similarly, subscribers can conceal their
15 activities by encrypting files. Thus, these files may need to be decrypted to detect
16 whether it constitutes an Item to be Seized.

17 23. I also believe that people engaged in crimes such as the one described
18 herein often use online accounts because they give people engaged in these crimes a way
19 to easily communicate with other co-conspirators. Moreover, online accounts are easily
20 concealed from law enforcement. Unlike physical documents, electronic documents can
21 be stored in a physical place far away, where they are less likely to be discovered.

22 24. Service providers typically retain certain transactional information about
23 the creation and use of each account on their systems. This information can include the
24

1 date on which the account was created, the length of service, records of log-in (i.e.,
2 session) times and durations, the types of service utilized, the status of the account
3 (including whether the account is inactive or closed), the methods used to connect to the
4 account (such as logging into the account via websites controlled by the Service
5 Provider), and other log files that reflect usage of the account. In addition, service
6 providers often have records of the Internet Protocol address ("IP address") used to
7 register the account and the IP addresses associated with particular logins to the
8 account. Because every device that connects to the Internet must use an IP address, IP
9 address information can help to identify which computers or other devices were used to
10 access the online account.

11 25. In some cases, subscribers will communicate directly with a service
12 provider about issues relating to the account, such as technical problems, billing
13 inquiries, or complaints from or about other users. Service providers typically retain
14 records about such communications, including records of contacts between the user and
15 the provider's support services, as well records of any actions taken by the provider or
16 user as a result of the communications.

17 26. In my training and experience, evidence of who was using an online account
18 may be found in address books, contact or buddy lists, emails in the account, and pictures
19 and files, whether stored as attachments or in the suite of the service provider's online
20 applications. Therefore, the computers of the Service Providers are likely to contain
21 stored electronic communications (including retrieved and un-retrieved email for their
22 subscribers) and information concerning subscribers and their use of the provider's
23
24

1 services, such as account access information, email transaction information, documents,
2 pictures, and account application information.

3 27. Microsoft maintains and offers its users the use of OneDrive. OneDrive is
4 a file-hosting service operated by Microsoft as part of its suite of online services. It allows
5 users to store files as well as other personal data like Windows settings or BitLocker
6 recovery keys in the cloud. Files can be synced to a PC and accessed from a web browser
7 or a mobile device, as well as shared publicly or with specific people. OneDrive offers 5
8 gigabytes of storage space free of charge; additional storage can be added either
9 separately or through subscriptions to other Microsoft services including Office 365 and
10 Groove Music.

11 28. Microsoft offers additional services that may be accessed in relation to and
12 share associated information with a user's email account, including: Office 365, Windows
13 Live Mail, Windows Live Writer, Windows Photo Gallery, Windows Live Messenger,
14 Microsoft Family Safety, and Microsoft Outlook Hotmail Connector.

15 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

16 29. Your Affiant anticipates executing these warrants under the Electronic
17 Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and
18 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government
19 copies of the records and other information (including the content of communications)
20 particularly described in Section I of Attachment "B." Upon receipt of the information
21 described in Section I of Attachment "B," government-authorized persons will review
22 that information to locate the items described in Section II of Attachment "B."
23
24

1 CONCLUSION

2 30. Based on the forgoing, I request that the Court issue the proposed search
3 warrant. This Court has jurisdiction to issue the requested warrant because it is "a court
4 of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A)
5 & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has
6 jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to
7 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the
8 service or execution of this warrant.

9 REQUEST FOR SEALING

10 31. I further request that the Court order that all papers in support of this
11 application, including the affidavit and search warrant, be sealed until further order of
12 the Court. These documents discuss an ongoing criminal investigation that is neither
13 public nor known to all of the targets of the investigation. Accordingly, there is good
14 cause to seal these documents because their premature disclosure may seriously
15 jeopardize that investigation.

16 Respectfully Submitted,

17 /s/
18 Zachary C. McKinney, Special Agent
19 Federal Bureau of Investigation

20 SWORN TO AND SUBSCRIBED
21 before me this 13th day of October 2017.

22 NANCY J. KOPPE
23 UNITED STATES MAGISTRATE JUDGE

I hereby attest and certify on 10/13/17
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.

NANCY J. KOPPE
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA

By [Signature] Deputy
Clerk

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "A-1"

ONLINE ACCOUNT TO BE SEARCHED

This warrant applies to information associated with the Microsoft email account centralpark1@live.com (the "Target Account 1") from inception to present, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.

1 ATTACHMENT "A-2"

2 ONLINE ACCOUNT TO BE SEARCHED

3 This warrant applies to information associated with the Microsoft email account
4 marilouroses@live.com (the "Target Account 2") from inception to present, which is
5 stored at premises owned, maintained, controlled, or operated by Microsoft Corporation,
6 headquartered at 1 Microsoft Way, Redmond, Washington, 98052.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachments A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachments A-1 and A-2 from account inception to present:

- a. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any OneDrive accounts associated with or assigned to Target Accounts 1 and 2.
- b. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Office 360 accounts associated with or assigned to Target Accounts 1 and 2.
- c. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Microsoft Family Safety accounts or services associated with or assigned to Target Accounts 1 and 2.
- d. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Writer accounts or services associated with or assigned to Target Accounts 1 and 2.
- e. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Mail accounts or services associated with or assigned to Target Accounts 1 and 2.
- f. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Photo Gallery accounts or services associated with or assigned to Target Accounts 1 and 2.
- g. The contents of all communications, transactions, records, documents, programs, or materials stored in or associated with any Windows Live Messenger accounts or services associated with or assigned to Target Accounts 1 and 2.

1 II. Information to be seized by the United States

2 After reviewing all information described in Section I, the United States will seize
3 evidence of violations of Title 18, United States Code Sections 32(a)
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
5 International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of
6 Firearms by Non Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject
7 Offenses") that occur in the form of the following, from account inception to present:

- 8 a. Communications, transactions and records that may establish ownership
9 and control (or the degree thereof) of the Target Account, including address
10 books, contact or buddy lists, bills, invoices, receipts, registration records,
11 bills, correspondence, notes, records, memoranda, telephone/address books,
12 photographs, video recordings, audio recordings, lists of names, records of
13 payment for access to newsgroups or other online subscription services, and
14 attachments to said communications, transactions and records.
- 15 b. Communications, transactions and records to/from persons who may be co-
16 conspirators of the Subject Offenses, or which may identify co-conspirators.
- 17 c. Communications, transactions and records which may show motivation to
18 commit the Subject Offenses.
- 19 d. Communications, transactions and records that relate to the Subject
20 Offenses.
- 21 e. The terms "communications," "transactions," "records," "documents,"
22 "programs," or "materials" include all information recorded in any form,
23 visual or aural, and by any means, whether in handmade form (including,
24 but not limited to, writings, drawings, paintings), photographic form
25 (including, but not limited to, pictures or videos), or electrical, electronic or
26 magnetic form, as well as digital data files. These terms also include any
27 applications (i.e. software programs). These terms expressly include, among
28 other things, Emails, instant messages, chat logs, correspondence attached
29 as to Emails (or drafts), calendar entries, buddy lists.

- a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. using hash values to narrow the scope of what may be found. Hash values are under-inclusive, but are still a helpful tool;
- f. scanning storage areas;
- g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and

1 (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later
2 off-site copying or review.

3 (f) Executing and Returning the Warrant.

4 (1) Warrant to Search for and Seize a Person or Property.

5 (B) Inventory. An officer present during the execution of the warrant must prepare and verify
6 an inventory of any property seized. . . . In a case involving the seizure of electronic storage media
7 or the seizure or copying of electronically stored information, the inventory may be limited to
8 describing the physical storage media that were seized or copied. The officer may retain a copy of
9 the electronically stored information that was seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in accordance with the
11 following:

12 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the
13 warrant, an agent is required to file an inventory return with the Court, that is, to file an
14 itemized list of the property seized. Execution of the warrant begins when the United States
15 serves the warrant on the named custodian; execution is complete when the custodian
16 provides all Search Warrant Data to the United States. Within fourteen (14) days of
17 completion of the execution of the warrant, the inventory will be filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the
19 electronically stored information must be seized after the issuance of the warrant and copied
20 after the execution of the warrant, not the "later review of the media or information" seized,
21 or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be
23 limited to a description of the "physical storage media" into which the Search Warrant Data
24 that was seized was placed, not an itemization of the information or data stored on the
"physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes
of the investigation. The government proposes that the original storage media on which the
Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be
retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any
information in the Search Warrant Data that is not set forth in Attachment B, Section II, that
information will be copied onto appropriate media and returned to the person from whom the
information was seized.

UNITED STATES DISTRICT COURT

for the
District of NevadaI hereby attest and certify on 10-3-17
that the foregoing document is a full true and correct
copy of the original on file in my office, and in my legal
custody.In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INSTAGRAM ACCOUNTS STORED AT
PREMISES CONTROLLED BY FACEBOOK
CORPORATION: Mariloudanleypaddock A 4Case No. 2:17-mj-0096
By [Signature] Deputy
SecretaryCAM FERENBACH
U.S. MAGISTRATE JUDGE
DISTRICT OF NEVADA

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the
property to be searched and give its location):INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION:
Mariloudanleypaddock A4located in the DEA District of , there is now concealed (identify the
person or describe the property to be seized):INSTAGRAM ACCOUNTS STORED AT PREMISES CONTROLLED BY FACEBOOK CORPORATION:
Mariloudanleypaddock A4

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
Title 26, United States Code, Section 5841.	Violation of National Firearms Act

The application is based on these facts:
I believe there is probable cause to believe that in the subject accounts listed in Attachments "A1", "A2", "A3",
"A4", "A5" there is proof that constitutes evidence of the commission of criminal offense(s); contraband, the fruits
of crime and things otherwise criminally possessed and been used as the means of committing criminal offense(s)

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

151
Applicant's signature

Printed name and title

Sworn to before me and signed in my presence.

Date: 10-3-17City and state: Las Vegas, Nevada

CAM FERENBACH

Judge's signature
CAM FERENBACH
U.S. MAGISTRATE JUDGE
Printed name and title

FILED
2017 OCT -3 PM 3:55
U.S. MAGISTRATE JUDGE
BY

1 ATTACHMENT "C"

2 PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
3 PURSUANT TO THIS SEARCH WARRANT

4 1. In executing this warrant, the government must make reasonable efforts to
5 use methods and procedures that will locate and expose in the electronic data produced
6 in response to this search warrant ("the Search Warrant Data") those categories of data,
7 files, documents, or other electronically stored information that are identified with
8 particularity in the warrant, while minimizing exposure or examination of irrelevant,
9 privileged, or confidential files to the extent reasonably practicable.

10 2. When the Search Warrant Data is received, the government will make a
11 duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The
12 original version of the Search Warrant Data will be sealed and preserved for purposes
13 of: later judicial review or order to return or dispose of the Search Warrant Data;
14 production to the defense in any criminal case if authorized by statute, rule, or the
15 Constitution; for purposes of showing the chain of custody of the Search Warrant Data
16 and the Search Warrant Data Copy; or for any other lawful purpose. The original of the
17 Search Warrant Data will not be searched or examined except to ensure that it has been
18 fully and completely replicated in the Search Warrant Data Copy.

19 3. The investigating agents will then search the entirety of the Search
20 Warrant Data Copy using any and all methods and procedures deemed appropriate by
21 the United States designed to identify the information listed as Information to be Seized
22 in Attachment B, Section II. The United States may copy, extract or otherwise segregate
23 information or data listed as Information to be Seized in Attachment B, Section II.
24 Information or data so copied, extracted or otherwise segregated will no longer be subject
to any handling restrictions that might be set out in this protocol beyond those required
by binding law. To the extent evidence of crimes not within the scope of this warrant
appear in plain view during this review, a supplemental or "piggyback" warrant will be
applied for in order to further search that document, data, or other item.

Once the Search Warrant Data Copy has been thoroughly and completely
examined for any document, data, or other items identified in Attachment B, Section II
as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject
to any further search or examination unless authorized by another search warrant or
other appropriate court order. The Search Warrant Data Copy will be held and preserved
for the same purposes identified above in Paragraph 2.

1 5. The search procedures utilized for this review are at the sole discretion of
2 the investigating and prosecuting authorities, and may include the following techniques
(the following is a non-exclusive list, as other search procedures may be used):

3 a. examination of all of the data contained in the Search Warrant Data to view
4 the data and determine whether that data falls within the items to be seized as set forth
herein;

5 b. searching for and attempting to recover from the Search Warrant Data any
6 deleted, hidden, or encrypted data to determine whether that data falls within the list
7 of items to be seized as set forth herein (any data that is encrypted and unreadable will
8 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

9 c. surveying various file directories and the individual files they contain;

10 d. opening files in order to determine their contents;

11 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

12 f. scanning storage areas;

13 g. performing keyword searches through all electronic storage areas to
14 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A1 and A2; and/or

15 h. performing any other data analysis technique that may be necessary to
16 locate and retrieve the evidence described in Attachment B, Section II.

17 Return and Review Procedures

18 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
19 part:

20 (e) Issuing the Warrant.

21 (2) Contents of the Warrant.

22 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
23 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
24 be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
4 copying of electronically stored information. Unless otherwise specified, the warrant
5 authorizes a later review of the media or information consistent with the warrant. The
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
7 on-site copying of the media or information, and not to any later off-site copying or
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare
9 and verify an inventory of any property seized. . . . In a case involving the seizure of
10 electronic storage media or the seizure or copying of electronically stored information,
11 the inventory may be limited to describing the physical storage media that were seized
12 or copied. The officer may retain a copy of the electronically stored information that was
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
15 of the warrant, an agent is required to file an inventory return with the Court, that is,
16 to file an itemized list of the property seized. Execution of the warrant begins when
17 the United States serves the warrant on the named custodian; execution is complete
18 when the custodian provides all Search Warrant Data to the United States. Within
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be
20 filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
19 which the electronically stored information must be seized after the issuance of the
20 warrant and copied after the execution of the warrant, not the "later review of the media
21 or information" seized, or the later off-site digital copying of that media.

20 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
21 may be limited to a description of the "physical storage media" into which the Search
22 Warrant Data that was seized was placed, not an itemization of the information or data
23 stored on the "physical storage media" into which the Search Warrant Data was placed;

- 1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
- 2 purposes of the investigation. The government proposes that the original storage media
- 3 on which the Search Warrant Data was placed plus a full image copy of the seized Search
- 4 Warrant Data be retained by the government.
- 5 e. If the person from whom any Search Warrant Data was seized requests the return
- 6 of any information in the Search Warrant Data that is not set forth in Attachment B,
- 7 Section II, that information will be copied onto appropriate media and returned to the
- 8 person from whom the information was seized.
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

UNITED STATES DISTRICT COURT

for the
District of Nevada

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))
 AMAZON ACCOUNT LINKED TO)
 CENTRA! PARK1@LIVE.COM THAT IS STORED AT A)
 PREMISES CONTROLLED BY AMAZON, INC.)

Case No. 2:17-mj- 972-NJK

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____ Nevada
 (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

YOU ARE COMMANDED to execute this warrant on or before October 20, 2017 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Nancy J. Koppe

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 10/16/2017 9:00 pmCity and state: Las Vegas, Nevada

Judge's signature

Printed name and title

ATTACHMENT "A"

ONLINE ACCOUNT TO BE SEARCHED

1. This warrant applies to information related to the Amazon.com account associated with centralpark1@live.com (the "Target Amazon Account") from its inception to present, which is stored at premises owned, maintained, controlled, or operated by Amazon.com, Inc., headquartered at 300 Deschutes Way SW, Suite 304, Tumwater, WA 98501.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "B"
Particular Things to be Seized

I. **Information to be disclosed by the Service Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of Amazon.com, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from account inception to present:

- a. All names, addresses, email addresses, shipping addresses, and billing information associated with the Target Amazon Account;
- b. Date of account creation;
- c. All purchase history;
- d. Service usage information;
- e. All Internet Protocol Address logs and information;
- f. All messages and/or communications exchanged with Amazon.com representative;
- g. Any and all information, files, and data in possession of Amazon.com and/or any other entities controlled or operation by Amazon.com, Inc. related to the Target Amazon Account.

II. **Information to be seized by the United States**

After reviewing all information described in Section I, the United States will seize evidence of violations of Title 18, United States Code Sections 32(a) (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at International Airport); and 922(a)(3); 5 (Unlawful Interstate Transport/Delivery of Firearms by Non Federal Firearms Licensee) (the "Subject Offenses") that occur in the form of the following, from account inception to present:

- a. Communications, transactions and records that may establish ownership and control (or the degree thereof) of the Target Account, including address books, contact or buddy lists, bills, invoices, receipts, registration records, bills, correspondence, notes, records, memoranda, telephone/address books, photographs, video recordings, audio recordings, lists of names, records of

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

payment for access to newsgroups or other online subscription services, and attachments to said communications, transactions and records.

- b. Communications, transactions and records to/from persons who may be co-conspirators of the Subject Offenses, or which may identify co-conspirators.
- c. Communications, transactions and records which may show motivation to commit the Subject Offenses.
- d. Communications, transactions and records that relate to the Subject Offenses.
- e. Information related to wire transfers and/or the movement, possession, or storage of currency and valuable items.

1 ATTACHMENT "C"

2 PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
3 PURSUANT TO THIS SEARCH WARRANT

4 1. In executing this warrant, the government must make reasonable efforts to
5 use methods and procedures that will locate and expose in the electronic data produced
6 in response to this search warrant ("the Search Warrant Data") those categories of data,
7 files, documents, or other electronically stored information that are identified with
8 particularity in the warrant, while minimizing exposure or examination of irrelevant,
9 privileged, or confidential files to the extent reasonably practicable.

10 2. When the Search Warrant Data is received, the government will make a
11 duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The
12 original version of the Search Warrant Data will be sealed and preserved for purposes
13 of: later judicial review or order to return or dispose of the Search Warrant Data;
14 production to the defense in any criminal case if authorized by statute, rule, or the
15 Constitution; for purposes of showing the chain of custody of the Search Warrant Data
16 and the Search Warrant Data Copy; or for any other lawful purpose. The original of the
17 Search Warrant Data will not be searched or examined except to ensure that it has been
18 fully and completely replicated in the Search Warrant Data Copy.

19 3. The investigating agents will then search the entirety of the Search
20 Warrant Data Copy using any and all methods and procedures deemed appropriate by
21 the United States designed to identify the information listed as Information to be Seized
22 in Attachment B, Section II. The United States may copy, extract or otherwise segregate
23 information or data listed as Information to be Seized in Attachment B, Section II.
24 Information or data so copied, extracted or otherwise segregated will no longer be subject
to any handling restrictions that might be set out in this protocol beyond those required
by binding law. To the extent evidence of crimes not within the scope of this warrant
appear in plain view during this review, a supplemental or "piggyback" warrant will be
applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely
examined for any document, data, or other items identified in Attachment B, Section II
as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject
to any further search or examination unless authorized by another search warrant or
other appropriate court order. The Search Warrant Data Copy will be held and preserved
for the same purposes identified above in Paragraph 2.

1 5. The search procedures utilized for this review are at the sole discretion of
2 the investigating and prosecuting authorities, and may include the following techniques
(the following is a non-exclusive list, as other search procedures may be used):

3 a. examination of all of the data contained in the Search Warrant Data to view
4 the data and determine whether that data falls within the items to be seized as set forth
herein;

5 b. searching for and attempting to recover from the Search Warrant Data any
6 deleted, hidden, or encrypted data to determine whether that data falls within the list
7 of items to be seized as set forth herein (any data that is encrypted and unreadable will
8 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

9 c. surveying various file directories and the individual files they contain;

10 d. opening files in order to determine their contents;

11 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

12 f. scanning storage areas;

13 g. performing keyword searches through all electronic storage areas to
14 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A; and/or

15 h. performing any other data analysis technique that may be necessary to
16 locate and retrieve the evidence described in Attachment B, Section II.

17 Return and Review Procedures

18 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

19 (e) Issuing the Warrant.

20 (2) Contents of the Warrant.

21 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
22 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
23 be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
4 copying of electronically stored information. Unless otherwise specified, the warrant
5 authorizes a later review of the media or information consistent with the warrant. The
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
7 on-site copying of the media or information, and not to any later off-site copying or
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare
9 and verify an inventory of any property seized. . . . In a case involving the seizure of
10 electronic storage media or the seizure or copying of electronically stored information,
11 the inventory may be limited to describing the physical storage media that were seized
12 or copied. The officer may retain a copy of the electronically stored information that was
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
15 of the warrant, an agent is required to file an inventory return with the Court, that is,
16 to file an itemized list of the property seized. Execution of the warrant begins when
17 the United States serves the warrant on the named custodian; execution is complete
18 when the custodian provides all Search Warrant Data to the United States. Within
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be
20 filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
19 which the electronically stored information must be seized after the issuance of the
20 warrant and copied after the execution of the warrant, not the "later review of the media
21 or information" seized, or the later off-site digital copying of that media.

20 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
21 may be limited to a description of the "physical storage media" into which the Search
22 Warrant Data that was seized was placed, not an itemization of the information or data
23 stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
2 purposes of the investigation. The government proposes that the original storage media
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return
5 of any information in the Search Warrant Data that is not set forth in Attachment B,
6 Section II, that information will be copied onto appropriate media and returned to the
7 person from whom the information was seized.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

1 STEVEN W. MYHRE
Acting United States Attorney
2 District of Nevada
CRISTINA D. SILVA
3 PATRICK BURNS
Assistant United States Attorneys
4 501 Las Vegas Blvd. South, Ste. 1100
Las Vegas, Nevada 89101
Telephone: (702) 388-6336
5 Fax (702) 388-6698
john.p.burns@usdoj.gov

6 Attorney for the United States of America

7
8 **UNITED STATES DISTRICT COURT**
DISTRICT OF NEVADA

9 -oOo-

10 IN THE MATTER OF THE SEARCH OF
INFORMATION RELATED TO THE
11 AMAZON ACCOUNT LINKED TO
CENTRALPARK1@LIVE.COM THAT IS
12 STORED AT A PREMISES
CONTROLLED BY AMAZON, INC.

Magistrate No. 17-mj-972-NSK

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH
WARRANT**

(Under Seal)

14 STATE OF NEVADA)
15) ss:
16 COUNTY OF CLARK)

17 **AFFIDAVIT IN SUPPORT OF AN**
APPLICATION FOR A SEARCH WARRANT

18 I, Ryan S. Burke, Special Agent, Federal Bureau of Investigation (FBI), having
19 been duly sworn, hereby depose and say:

20 **INTRODUCTION AND AGENT BACKGROUND**

21 1. Your Affiant makes this affidavit in support of an application for a search
22 warrant for information related to the Amazon account associated with email account
23 centralpark1@live.com ("Target Amazon Account"). The Target Amazon Account is
24

1 associated with STEPHEN PADDOCK and the information is stored at a premises
2 owned, maintained, controlled, or operated by Amazon.com, Inc. ("Amazon"), an
3 American electronic commerce and cloud computing company based in Tumwater,
4 Washington. More generally, Amazon is a website that allows account holders to browse
5 for and purchase a variety of goods. Separately, Amazon offers and provides internet-
6 based cloud services to various individuals/entities. The information to be searched is
7 described in the following paragraphs and in Attachment "A" (attached hereto and
8 incorporated herein by reference). This affidavit is made in support of an application for
9 a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require
10 Amazon to disclose to the government records and other information in its possession,
11 pertaining to the subscriber or customer associated with the Target Amazon Account.

12 2. I am an "investigative or law enforcement officer of the United States"
13 within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of
14 the United States who is empowered by law to conduct investigations of, and to make
15 arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

16 3. I have been employed as a Special Agent of the FBI for approximately five
17 years, which began at the FBI Academy in October 2012. Upon completion of the
18 academy, I was transferred to the Las Vegas Division's white collar crime squad and
19 then the human trafficking squad. Since October 2015, I have been assigned to the Las
20 Vegas Division's violent crime/gang squad. Additionally, I have been a certified member
21 of the FBI's Cellular Analysis Survey Team since August 2015 due to my expertise in
22 the field of historical cell site analysis.

1 4. During my tenure with the FBI, I have conducted surveillance, analyzed
2 telephone records, interviewed witnesses, supervised activities of sources, executed
3 search warrants, executed arrest warrants, and participated in court-authorized
4 interceptions of wire and electronic communications. These investigative activities have
5 been conducted in conjunction with a variety of investigations, to include those involving
6 robbery, drug trafficking, kidnapping, murder, criminal enterprises, and more. In
7 addition to my practical experiences, I received five months of extensive law enforcement
8 training at the FBI Academy.

9 5. The facts in this affidavit are derived from your Affiant's personal
10 observations, his training and experience, and information obtained from other agents,
11 detectives, and witnesses. This affidavit is intended to show merely that there is
12 sufficient probable cause for the requested warrant and does not set forth all of the
13 Affiant's knowledge about this matter.

14 6. Based on your Affiant's training and experience and the facts as set forth
15 in this affidavit, there is probable cause to believe that violations of:

- 16 a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C.A. § 32(a);
17 b. Violence at International Airport - 18 U.S.C. § 37(a)(2); and
18 c. Unlawful Interstate Transport/Delivery of Firearms by Non Federal
19 Firearms Licensee - 18 USC 922(a)(3) and (5).

20 (hereafter, "Subject Offenses") have been committed by STEPHEN PADDOCK and
21 others yet unknown. There is also probable cause to search the information described in
22 Attachment "A" for evidence of these crimes and information which might reveal the
23
24

1 identities of others involved in these crimes, as described in Attachment "B" (attached
2 hereto and incorporated herein by reference).

3 **PROBABLE CAUSE**

4 7. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music
5 festival, was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At
6 approximately 10:08 p.m., the Las Vegas Metropolitan Police Department (LVMPD)
7 received calls reporting shots had been fired at the concert and multiple victims were
8 struck. LVMPD determined the shots were coming from Rooms 134 and 135 on the 32nd
9 floor of the Mandalay Bay Resort and Casino, located due west of the festival grounds at
10 3950 South Las Vegas Boulevard, Las Vegas, Nevada. These rooms are an elevated
11 position which overlooks the concert venue. Witness statements and video
12 footage captured during the attack indicates that the weapons being used were firing in
13 a fully-automatic fashion.

14 8. LVMPD officers ultimately made entry into the room and located an
15 individual later identified as STEPHEN PADDOCK. Paddock was deceased from an
16 apparent self-inflicted gunshot wound.

17 9. Paddock's Nevada driver's license was located in the Mandalay Bay hotel
18 room with Paddock, and both hotel rooms were registered in his name. A player's club
19 card in name of Marilou Danley was located in Paddock's room, and the card returned
20 to the address located on Babbling Brook Street in Mesquite, Nevada. FBI Agents
21 located Danley, who was traveling outside the United States at the time of the
22 shooting. It was ultimately determined that Danley resided with Paddock at the
23 Babbling Brook address.

1 10. On October 2, 2017, search warrants were executed on Paddock's Mandalay
2 Bay hotel rooms, Paddock's vehicle at Mandalay Bay, and two Nevada residences owned
3 by Paddock: 1372 Babbling Brook Court in Mesquite, and 1735 Del Webb Parkway in
4 Reno, Nevada. Officers and Agents found over 20 firearms, hundreds of rounds of
5 ammunition, and hundreds of spent shell casings in the Mandalay Bay hotel rooms, in
6 close proximity to Paddock's body. Over a thousand rounds of rifle ammunition and 100
7 pounds of explosive material were found in Paddock's vehicle. Additional explosive
8 material, approximately 18 firearms, and over 1,000 rounds of ammunition were located
9 at the Mesquite residence. A large quantity of ammunition and multiple firearms were
10 recovered from the Reno residence.

11 11. As of this date, 58 people have been identified to have been killed in
12 Paddock's attack and another 557 were reportedly injured. Additionally, investigators
13 discovered that STEPHEN PADDOCK also utilized a firearm to shoot large fuel tanks
14 on Las Vegas McCarran International Airport property. Multiple bullet holes were found
15 on the tank, which investigators believe was an attempt by STEPHEN PADDOCK to
16 cause the tanks to explode.

17 12. In an effort to determine whether or not STEPHEN PADDOCK was
18 assisted and/or conspired with unknown individuals, investigators have attempted to
19 identify all of STEPHEN PADDOCK's communication facilities. Based on a review of his
20 financial accounts, email address centralpark1@live.com ("Email Account") was
21 determined to belong to STEPHEN PADDOCK. On October 3, 2017, investigators
22 requested an emergency disclosure of records from Microsoft related to the Email
23 Account so it could be searched for any evidence of additional co-conspirators. Within
24

1 the Email Account, investigators identified the Target Amazon Account as one that
2 required further investigation.

3 13. Numerous emails sent from Amazon to the Email Account were discovered
4 in the Email Account which were addressed by Amazon to "Stephen" and listed
5 STEPHEN PADDOCK's residence in Mesquite, Nevada as the shipping destination. For
6 these reasons in conjunction with the Target Amazon Account being associated with the
7 Email Account, investigators strongly believe the Target Amazon Account was controlled
8 and operated by STEPHEN PADDOCK.

9 14. On September 7, 2017, the Email Account received an email relating to the
10 Target Amazon Account's purchase of an EOTech 512.A65 Tactical Holographic firearm
11 accessory. Within the email, which was addressed to STEPHEN PADDOCK, Amazon
12 confirmed the firearm accessory would be delivered to STEPHEN PADDOCK's
13 residence. Investigators believe this piece of equipment was utilized in the attack carried
14 out by STEPHEN PADDOCK.

15 15. Your Affiant believes the requested search warrant will yield significant
16 information from Amazon such as STEPHEN PADDOCK's search history, purchase
17 history, IP addresses, shipping addresses, payment information, and more, which may
18 constitute evidence of his planning of the attack and potentially identify other
19 participants in the attack. Ultimately, your Affiant strongly believes the requested
20 information will lead investigators to determine the full scope of STEPHEN PADDOCK's
21 plan and/or conspiracy.

22 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**
23
24

16. Your Affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Amazon to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment "B." Upon receipt of the information described in Section I of Attachment "B," government-authorized persons will review that information to locate the items described in Section II of Attachment "B."

CONCLUSION

17. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

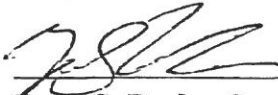
REQUEST FOR SEALING

18. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good

///

1 cause to seal these documents because their premature disclosure may seriously
2 jeopardize that investigation.
3
4

5 Respectfully Submitted,

6 

7 Ryan S. Burke, Special Agent
8 Federal Bureau of Investigation

9 SWORN TO AND SUBSCRIBED
10 before me this 4th day of October 2017.

11 

12 UNITED STATES MAGISTRATE JUDGE
13
14
15
16
17
18
19
20
21
22
23
24

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Amazon.com, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from account inception to present:

- a. All names, addresses, email addresses, shipping addresses, and billing information associated with the Target Amazon Account;
- b. Date of account creation;
- c. All purchase history;
- d. Service usage information;
- e. All Internet Protocol Address logs and information;
- f. All messages and/or communications exchanged with Amazon.com representative;
- g. Any and all information, files, and data in possession of Amazon.com and/or any other entities controlled or operation by Amazon.com, Inc. related to the Target Amazon Account.

II. Information to be seized by the United States

After reviewing all information described in Section I, the United States will seize evidence of violations of Title 18, United States Code Sections 32(a) (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at International Airport); and 922(a)(3); 5 (Unlawful Interstate Transport/Delivery of Firearms by Non Federal Firearms Licensee) (the "Subject Offenses") that occur in the form of the following, from account inception to present:

- a. Communications, transactions and records that may establish ownership and control (or the degree thereof) of the Target Account, including address books, contact or buddy lists, bills, invoices, receipts, registration records, bills, correspondence, notes, records, memoranda, telephone/address books, photographs, video recordings, audio recordings, lists of names, records of

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

payment for access to newsgroups or other online subscription services, and attachments to said communications, transactions and records.

- b. Communications, transactions and records to/from persons who may be co-conspirators of the Subject Offenses, or which may identify co-conspirators.
- c. Communications, transactions and records which may show motivation to commit the Subject Offenses.
- d. Communications, transactions and records that relate to the Subject Offenses.
- e. Information related to wire transfers and/or the movement, possession, or storage of currency and valuable items.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "C"

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

**PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT**

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

1 5. The search procedures utilized for this review are at the sole discretion of
2 the investigating and prosecuting authorities, and may include the following techniques
(the following is a non-exclusive list, as other search procedures may be used):

3 a. examination of all of the data contained in the Search Warrant Data to view
4 the data and determine whether that data falls within the items to be seized as set forth
herein;

5 b. searching for and attempting to recover from the Search Warrant Data any
6 deleted, hidden, or encrypted data to determine whether that data falls within the list
7 of items to be seized as set forth herein (any data that is encrypted and unreadable will
not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
8 (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

9 c. surveying various file directories and the individual files they contain;

10 d. opening files in order to determine their contents;

11 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

12 f. scanning storage areas;

13 g. performing keyword searches through all electronic storage areas to
14 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A; and/or

15 h. performing any other data analysis technique that may be necessary to
16 locate and retrieve the evidence described in Attachment B, Section II.

17 **Return and Review Procedures**

18 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

19 (e) Issuing the Warrant.

20 (2) Contents of the Warrant.

21 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
22 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
23 be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
4 copying of electronically stored information. Unless otherwise specified, the warrant
5 authorizes a later review of the media or information consistent with the warrant. The
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
7 on-site copying of the media or information, and not to any later off-site copying or
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare
9 and verify an inventory of any property seized. . . . In a case involving the seizure of
10 electronic storage media or the seizure or copying of electronically stored information,
11 the inventory may be limited to describing the physical storage media that were seized
12 or copied. The officer may retain a copy of the electronically stored information that was
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
15 of the warrant, an agent is required to file an inventory return with the Court, that is,
16 to file an itemized list of the property seized. Execution of the warrant begins when
17 the United States serves the warrant on the named custodian; execution is complete
18 when the custodian provides all Search Warrant Data to the United States. Within
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be
20 filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
19 which the electronically stored information must be seized after the issuance of the
20 warrant and copied after the execution of the warrant, not the "later review of the media
21 or information" seized, or the later off-site digital copying of that media.

21 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
22 may be limited to a description of the "physical storage media" into which the Search
23 Warrant Data that was seized was placed, not an itemization of the information or data
24 stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
2 purposes of the investigation. The government proposes that the original storage media
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return
5 of any information in the Search Warrant Data that is not set forth in Attachment B,
6 Section II, that information will be copied onto appropriate media and returned to the
7 person from whom the information was seized.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

UNITED STATES DISTRICT COURT

for the
District of Nevada

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

EMAIL ACCOUNT CENTRALPARK4804@GMAIL.COM

Case No. 2:17-mj- 970-NJK

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

YOU ARE COMMANDED to execute this warrant on or before October 20, 2017 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Nancy J. Koppe
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 10/6/2017 4:30 pm

City and state: Las Vegas, Nevada

Nancy J. Koppe
Judge's signature
Nancy J. Koppe US Magistrate Judge
Printed name and title

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "A"

ONLINE ACCOUNT TO BE SEARCHED

1. This warrant applies to information associated with the Google email account centralpark4804@gmail.com (the "Target Account") from its inception to present, which is stored at premises owned, maintained, controlled, or operated by Google, Inc., headquartered at 1600 Amphitheatre Way, Mountain View, California, 94043.

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from account inception to present:

- a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
- d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
- e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Google-related facility.

1 II. Information to be seized by the United States

2 After reviewing all information described in Section I, the United States will seize
3 evidence of violations of Title 18, United States Code Sections 32(a)
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
5 International Airport); and 922(a)(3); 5 (Unlawful Interstate Transport/Delivery of
Firearms by Non Federal Firearms Licensee) (the "Subject Offenses") that occur in the
form of the following, from account inception to present:

- 6 a. Communications, transactions and records that may establish ownership
7 and control (or the degree thereof) of the Target Account, including address
8 books, contact or buddy lists, bills, invoices, receipts, registration records,
9 bills, correspondence, notes, records, memoranda, telephone/address books,
10 photographs, video recordings, audio recordings, lists of names, records of
11 payment for access to newsgroups or other online subscription services, and
12 attachments to said communications, transactions and records.
- 13 b. Communications, transactions and records to/from persons who may be co-
14 conspirators of the Subject Offenses, or which may identify co-conspirators.
- 15 c. Communications, transactions and records which may show motivation to
16 commit the Subject Offenses.
- 17 d. Communications, transactions and records that relate to the Subject
18 Offenses.
- 19 e. The terms "communications," "transactions," "records," "documents,"
20 "programs," or "materials" include all information recorded in any form,
21 visual or aural, and by any means, whether in handmade form (including,
22 but not limited to, writings, drawings, paintings), photographic form
23 (including, but not limited to, pictures or videos), or electrical, electronic or
24 magnetic form, as well as digital data files. These terms also include any
applications (i.e. software programs). These terms expressly include, among
other things, Emails, instant messages, chat logs, correspondence attached
as to Emails (or drafts), calendar entries, buddy lists.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "C"

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

**PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT**

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

1 5. The search procedures utilized for this review are at the sole discretion of
2 the investigating and prosecuting authorities, and may include the following techniques
(the following is a non-exclusive list, as other search procedures may be used):

3 a. examination of all of the data contained in the Search Warrant Data to view
4 the data and determine whether that data falls within the items to be seized as set forth
herein;

5 b. searching for and attempting to recover from the Search Warrant Data any
6 deleted, hidden, or encrypted data to determine whether that data falls within the list
7 of items to be seized as set forth herein (any data that is encrypted and unreadable will
8 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

9 c. surveying various file directories and the individual files they contain;

10 d. opening files in order to determine their contents;

11 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

12 f. scanning storage areas;

13 g. performing keyword searches through all electronic storage areas to
14 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A; and/or

15 h. performing any other data analysis technique that may be necessary to
16 locate and retrieve the evidence described in Attachment B, Section II.

17 **Return and Review Procedures**

18 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

19 (e) Issuing the Warrant.

20 (2) Contents of the Warrant.

21 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
22 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
23 be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
4 copying of electronically stored information. Unless otherwise specified, the warrant
5 authorizes a later review of the media or information consistent with the warrant. The
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
7 on-site copying of the media or information, and not to any later off-site copying or
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare
9 and verify an inventory of any property seized. . . . In a case involving the seizure of
10 electronic storage media or the seizure or copying of electronically stored information,
11 the inventory may be limited to describing the physical storage media that were seized
12 or copied. The officer may retain a copy of the electronically stored information that was
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
15 of the warrant, an agent is required to file an inventory return with the Court, that is,
16 to file an itemized list of the property seized. Execution of the warrant begins when
17 the United States serves the warrant on the named custodian; execution is complete
18 when the custodian provides all Search Warrant Data to the United States. Within
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be
20 filed.

21 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
22 which the electronically stored information must be seized after the issuance of the
23 warrant and copied after the execution of the warrant, not the "later review of the media
24 or information" seized, or the later off-site digital copying of that media.

25 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
26 may be limited to a description of the "physical storage media" into which the Search
27 Warrant Data that was seized was placed, not an itemization of the information or data
28 stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
2 purposes of the investigation. The government proposes that the original storage media
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return
5 of any information in the Search Warrant Data that is not set forth in Attachment B,
6 Section II, that information will be copied onto appropriate media and returned to the
7 person from whom the information was seized.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

1 STEVEN W. MYHRE
Acting United States Attorney
2 District of Nevada
CRISTINA D. SILVA
3 PATRICK BURNS
Assistant United States Attorneys
501 Las Vegas Blvd. South, Ste. 1100
4 Las Vegas, Nevada 89101
Telephone: (702) 388-6336
5 Fax (702) 388-6698
john.p.burns@usdoj.gov

6 Attorney for the United States of America

7
8 **UNITED STATES DISTRICT COURT**
DISTRICT OF NEVADA

9 -oOo-

10 IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
11 EMAIL ACCOUNT
CENTRALPARK4804@GMAIL.COM
12 THAT IS STORED AT A PREMISES
CONTROLLED BY GOOGLE.

Magistrate No. 17-mj-970-NJK

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH
WARRANT**

(Under Seal)

14 STATE OF NEVADA)
15) ss:
16 COUNTY OF CLARK)

17 **AFFIDAVIT IN SUPPORT OF AN**
APPLICATION FOR A SEARCH WARRANT

18 I, Ryan S. Burke, Special Agent, Federal Bureau of Investigation (FBI), having
19 been duly sworn, hereby depose and say:

20 **INTRODUCTION AND AGENT BACKGROUND**

21 1. Your Affiant makes this affidavit in support of an application for a search
22 warrant for information associated with email account centralpark4804@gmail.com
23 ("Target Account"), an account associated with STEPHEN PADDOCK, that is stored at
24

1 a premises owned, maintained, controlled, or operated by Google, Inc. ("Google"), an
2 American multinational technology based in Mountain View, California that specializes
3 in Internet-related services and products. Those services include, but are not limited to,
4 online advertising technologies, a search engine, email services, cloud computing, and
5 many other services. The information to be searched is described in the following
6 paragraphs and in Attachment "A" (attached hereto and incorporated herein by
7 reference). This affidavit is made in support of an application for a search warrant under
8 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the
9 government records and other information in its possession, pertaining to the subscriber
10 or customer associated with the Target Account.

11 2. I am an "investigative or law enforcement officer of the United States"
12 within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of
13 the United States who is empowered by law to conduct investigations of, and to make
14 arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

15 3. I have been employed as a Special Agent of the FBI for approximately five
16 years, which began at the FBI Academy in October 2012. Upon completion of the
17 academy, I was transferred to the Las Vegas Division's white collar crime squad and
18 then the human trafficking squad. Since October 2015, I have been assigned to the Las
19 Vegas Division's violent crime/gang squad. Additionally, I have been a certified member
20 of the FBI's Cellular Analysis Survey Team since August 2015 due to my expertise in
21 the field of historical cell site analysis.

22 4. During my tenure with the FBI, I have conducted surveillance, analyzed
23 telephone records, interviewed witnesses, supervised activities of sources, executed
24

1 search warrants, executed arrest warrants, and participated in court-authorized
2 interceptions of wire and electronic communications. These investigative activities have
3 been conducted in conjunction with a variety of investigations, to include those involving
4 robbery, drug trafficking, kidnapping, murder, criminal enterprises, and more. In
5 addition to my practical experiences, I received five months of extensive law enforcement
6 training at the FBI Academy.

7 5. The facts in this affidavit are derived from your Affiant's personal
8 observations, his training and experience, and information obtained from other agents,
9 detectives, and witnesses. This affidavit is intended to show merely that there is
10 sufficient probable cause for the requested warrant and does not set forth all of the
11 Affiant's knowledge about this matter.

12 6. Based on your Affiant's training and experience and the facts as set forth
13 in this affidavit, there is probable cause to believe that violations of:

- 14 a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C.A. § 32(a);
- 15 b. Violence at International Airport - 18 U.S.C. § 37(a)(2); and
- 16 c. Unlawful Interstate Transport/Delivery of Firearms by Non Federal
17 Firearms Licensee - 18 USC 922(a)(3) and (5).

18 (hereafter, "Subject Offenses") have been committed by STEPHEN PADDOCK and
19 others yet unknown. There is also probable cause to search the information described in
20 Attachment "A" for evidence of these crimes and information which might reveal the
21 identities of others involved in these crimes, as described in Attachment "B" (attached
22 hereto and incorporated herein by reference).

23 ///

PROBABLE CAUSE

7. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music festival, was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At approximately 10:08 p.m., the Las Vegas Metropolitan Police Department (LVMPD) received calls reporting shots had been fired at the concert and multiple victims were struck. LVMPD determined the shots were coming from Rooms 134 and 135 on the 32nd floor of the Mandalay Bay Resort and Casino, located due west of the festival grounds at 3950 South Las Vegas Boulevard, Las Vegas, Nevada. These rooms are an elevated position which overlooks the concert venue. Witness statements and video footage captured during the attack indicates that the weapons being used were firing in a fully-automatic fashion.

8. LVMPD officers ultimately made entry into the room and located an individual later identified as Stephen Paddock. Paddock was deceased from an apparent self-inflicted gunshot wound.

9. Paddock's Nevada driver's license was located in the Mandalay Bay hotel room with Paddock, and both hotel rooms were registered in his name. A player's club card in name of Marilou Danley was located in Paddock's room, and the card returned to the address located on Babbling Brook Street in Mesquite, Nevada. FBI Agents located Danley, who was traveling outside the United States at the time of the shooting. It was ultimately determined that Danley resided with Paddock at the Babbling Brook address.

10. On October 2, 2017, search warrants were executed on Paddock's Mandalay Bay hotel rooms, Paddock's vehicle at Mandalay Bay, and two Nevada residences owed

1 by Paddock: 1372 Babbling Brook Court in Mesquite, and 1735 Del Webb Parkway in
2 Reno, Nevada. Officers and Agents found over 20 firearms, hundreds of rounds of
3 ammunition, and hundreds of spent shell casings in the Mandalay Bay hotel rooms, in
4 close proximity to Paddock's body. Over a thousand rounds of rifle ammunition and 100
5 pounds of explosive material was found in Paddock's vehicle. Additional explosive
6 material, approximately 18 firearms, and over 1,000 rounds of ammunition was located
7 at the Mesquite residence. A large quantity of ammunition and multiple firearms were
8 recovered from the Reno residence.

9 11. As of this date, 58 people have been identified to have been killed in
10 Paddock's attack and another 557 were reportedly injured. Additionally, investigators
11 discovered that STEPHEN PADDOCK also utilized a firearm to shoot large fuel tanks
12 on Las Vegas McCarran International Airport property. Multiple bullet holes were found
13 on the tank, which investigators believe was an attempt by STEPHEN PADDOCK to
14 cause the tanks to explode.

15 12. In an effort to determine whether or not STEPHEN PADDOCK was
16 assisted and/or conspired with unknown individuals, investigators have attempted to
17 identify all of STEPHEN PADDOCK's communication facilities. Based on a review of his
18 financial accounts, email address centralpark1@live.com ("Account 2") was determined
19 to belong to STEPHEN PADDOCK. On October 3, 2017, investigators requested an
20 emergency disclosure of records from Microsoft related to Account 2 so it could be
21 searched for any evidence of additional co-conspirators. Within the account,
22 investigators identified the Target Account as one that required further investigation.

1 13. On July 6, 2017, the Target Account sent an email to Account 2 that read,
2 "try an ar before u buy. we have huge selection. located in the las vegas area." Later that
3 day, Account 2 sent an email to the Target Account that read, "we have a wide variety
4 of optics and ammunition to try." And lastly, Account 2 later sent an email to the Target
5 Account that read, "for a thrill try out bumpfire ar's with a 100 round magazine."

6 14. Based on the similarity of both email account names, investigators believe
7 the Target Account may also be controlled by STEPHEN PADDOCK. Additionally,
8 STEPHEN PADDOCK was previously a manager of an apartment complex in the Reno,
9 Nevada area called "Central Park," which investigators believe further substantiates his
10 association to the Target Account. However, investigators have been unable to figure out
11 why STEPHEN PADDOCK would be exchanging messages related to weapons that were
12 utilized in the attack between two of his email accounts. Conversely, if the Target
13 Account was not controlled by STEPHEN PADDOCK, investigators need to determine
14 who was communicating with him about weapons that were used in the attack. Paddock
15 acquired a substantial amount of firearms from out of state which appear to have been
16 transported into the state of Nevada where he resides.

17 15. Your Affiant believes the requested search warrant will yield significant
18 information from Google such as STEPHEN PADDOCK's contact list, email message
19 content, IP address usage, photographs, third-party applications associated with the
20 account, and more, which may constitute evidence of his planning of the attack and
21 potentially identify other participants in the attack. Ultimately, your Affiant strongly
22 believes the requested information will lead investigators to determine the full scope of
23 STEPHEN PADDOCK's plan.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

2 16. The following non-exhaustive list of definitions applies to this Affidavit and
3 the Attachments to this Affidavit:

a. The "Internet" is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web is a functionality of the Internet which allows users of the Internet to share information.

b. "Internet Service Providers" are companies that provide access to the Internet. ISPs can also provide other services for their customers including website hosting, email service, remote storage, and co-location of computers and other communications equipment. ISPs offer different ways to access the Internet including telephone-based (dial-up), broadband-based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data (bandwidth). Many ISPs assign each subscriber an account name, such as a user name, an email address, and an email mailbox, and the subscriber typically creates a password for his/her account.

c. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often in the form of log files), emails, information concerning content uploaded and/or stored on the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs

1 reserve and/or maintain computer disk storage space on their computer system for their
2 subscribers' use. This service by ISPs allows for both temporary and long-term storage
3 of electronic communications and many other types of electronic data and files.

4 d. "Online service providers" (also referred to here as "service
5 providers") are companies that provide online services such as email, chat or instant
6 messaging, word processing applications, spreadsheet applications, presentation
7 applications similar to PowerPoint, online calendar, photo storage and remote storage
8 services. Sometimes they also can provide web hosting, remote storage, and co-location
9 of computers and other communications equipment. Typically, each service provider
10 assigns each subscriber an account name, such as a user name or screen name and the
11 subscriber typically creates a password for his/her account.

12 e. "Computer," as used herein, is defined as "an electronic, magnetic,
13 optical, electrochemical, or other high speed data processing device performing logical or
14 storage functions, and includes any data storage facility or communications facility
15 directly related to or operating in conjunction with such device."

16 f. A "server" is a centralized computer that provides services for other
17 computers connected to it via a network. The other computers attached to a server are
18 sometimes called "clients." For example, in a large company, it is common for individual
19 employees to have client computers at their desktops. When the employees access their
20 email, or access files stored on the network itself, those files are pulled electronically
21 from the server, where they are stored, and are sent to the client's computer via the
22 network. Notably, servers can be physically stored in any location: it is not uncommon
23
24

1 for a network's server to be located hundreds (and even thousands) of miles away from
2 the client computers.

3 g. "Internet Protocol address," or "IP address," refers to a unique
4 number used by a computer to access the Internet. IP addresses can be dynamic,
5 meaning that the Internet Service Provider (ISP) assigns a different unique number to
6 a computer every time it accesses the Internet. IP addresses might also be static, that
7 is, an ISP assigns a user's computer a particular IP address which is used each time the
8 computer accesses the Internet.

9 h. The term "domain" refers to a word used as a name for computers,
10 networks, services, etc. A domain name typically represents a website, a server computer
11 that hosts that website, or even some computer (or other digital device) connected to the
12 internet. Essentially, when a website (or a server computer that hosts that website) is
13 connected to the internet, it is assigned an IP address. Because IP addresses are difficult
14 for people to remember, domain names are instead used because they are easier to
15 remember than IP addresses. Domain names are formed by the rules and procedures of
16 the Domain Name System (DNS). A common top level domain under these rules is ".com"
17 for commercial organizations, ".gov" for the United States government, and ".org" for
18 organizations. For example, www.usdoj.gov is the domain name that identifies a server
19 used by the U.S. Department of Justice, and which uses IP address of 149.101.46.71.

20 i. "Web hosting services" maintain server computers connected to the
21 Internet. Their customers use those computers to operate websites on the Internet.
22 Customers of web hosting companies place files, software code, databases, and other data
23
24

1 on servers. To do this, customers typically connect from their own computers to the
2 server computers across the Internet.

3 j. The term "WhoIs" lookup refers to a search of a publicly available
4 online database that lists information provided when a domain is registered or when an
5 IP address is assigned.

6 k. The terms "communications," "records," "documents," "programs," or
7 "materials" include all information recorded in any form, visual or aural, and by any
8 means, whether in handmade form (including, but not limited to, writings, drawings,
9 paintings), photographic form (including, but not limited to, pictures or videos), or
10 electrical, electronic or magnetic form, as well as digital data files. These terms also
11 include any applications (i.e. software programs). These terms expressly include, among
12 other things, emails, instant messages, chat logs, correspondence attached as to emails
13 (or drafts), calendar entries, buddy lists.

14 l. "Chat" is usually a real time electronic communication between two
15 or more individuals. Unlike email, which is frequently sent, then read and responded to
16 minutes, hours, or even days later, chats frequently involve an immediate conversation
17 between individuals, similar to a face-to-face conversation. Nearly all chat programs are
18 capable of saving the chat transcript, to enable users to preserve a record of the
19 conversation. By default, some chat programs have this capability enabled, while others
20 do not. Many popular web-based email providers, like Google and Google, provide chat
21 functionality as part of the online services they provide to account holders.

22 ///

23 ///

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

15
16
17
18
19
20
21
22
23

24

1 19. In general, when a subscriber receives an email, it is typically stored in the
2 subscriber's "mail box" on that service provider's servers until the subscriber deletes the
3 Email. If the subscriber does not delete the message, the message (and any attachments)
4 can remain on that service provider's servers indefinitely.

5 20. Similarly, when the subscriber sends an email, it is initiated at the
6 subscriber's computer, transferred via the Internet to the service provider's servers, and
7 then transmitted to its end destination. That service provider often saves a copy of the
8 email sent. Unless the sender of the email specifically deletes the Email from the
9 provider's server, the email can remain on the system indefinitely.

10 21. A sent or received email typically includes the content of the message,
11 source and destination addresses, the date and time at which the email was sent, and
12 the size and length of the email. If an email user writes a draft message but does not
13 send it, that message may also be saved by that service provider, but may not include all
14 of these categories of data.

15 22. Just as a computer on a desk can be used to store a wide variety of files, so
16 can online accounts, such as the accounts subject to this application. First, subscribers
17 can store many types of files as attachments to emails in online accounts. Second,
18 because service providers provide the services listed above (e.g. word processing,
19 spreadsheets, pictures), subscribers who use these services usually store documents on
20 servers maintained and/or owned by service providers. Thus, these online accounts often
21 contain documents such as pictures, audio or video recordings, logs, spreadsheets,
22 applications and other files.

1 23. Reviewing files stored in online accounts raises many of the same
2 difficulties as with reviewing files stored on a local computer. For example, based on my
3 training, my experience and this investigation, I know that subscribers of these online
4 services can conceal their activities by altering files before they upload them to the online
5 service. Subscribers can change file names to more innocuous sounding names (e.g.
6 renaming "FraudRecords.doc" to "ChristmasList.doc"), they can change file extensions
7 to make one kind of file appear like a different type of file (e.g. changing the spreadsheet
8 "StolenCreditProfiles.xls" to "FamilyPhoto.jpg" to appear to be a picture file, where the
9 file extension ".xls" denotes an Excel spreadsheet file and ".jpg" a JPEG format image
10 file), or they can change the times and dates a file was last accessed or modified by
11 changing a computer's system time/date and then uploading that file to the Online
12 Accounts. Thus, to detect any files that the subscriber may have concealed, agents will
13 need to review all of the files in the Target Account; they will, however, only seize the
14 items that the Court authorizes to be seized. Similarly, subscribers can conceal their
15 activities by encrypting files. Thus, these files may need to be decrypted to detect
16 whether it constitutes an Item to be Seized.

17 24. I also believe that people engaged in crimes such as the one described
18 herein often use online accounts because they give people engaged in these crimes a way
19 to easily communicate with other co-conspirators. Moreover, online accounts are easily
20 concealed from law enforcement. Unlike physical documents, electronic documents can
21 be stored in a physical place far away, where they are less likely to be discovered.

22 25. Service providers typically retain certain transactional information about
23 the creation and use of each account on their systems. This information can include the
24

1 date on which the account was created, the length of service, records of log-in (i.e.,
2 session) times and durations, the types of service utilized, the status of the account
3 (including whether the account is inactive or closed), the methods used to connect to the
4 account (such as logging into the account via websites controlled by the Service
5 Provider), and other log files that reflect usage of the account. In addition, service
6 providers often have records of the Internet Protocol address ("IP address") used to
7 register the account and the IP addresses associated with particular logins to the
8 account. Because every device that connects to the Internet must use an IP address, IP
9 address information can help to identify which computers or other devices were used to
10 access the online account.

11 26. In some cases, subscribers will communicate directly with a service
12 provider about issues relating to the account, such as technical problems, billing
13 inquiries, or complaints from or about other users. Service providers typically retain
14 records about such communications, including records of contacts between the user and
15 the provider's support services, as well records of any actions taken by the provider or
16 user as a result of the communications.

17 27. In my training and experience, evidence of who was using an online
18 account may be found in address books, contact or buddy lists, emails in the account,
19 and pictures and files, whether stored as attachments or in the suite of the service
20 provider's online applications. Therefore, the computers of the Service Providers are
21 likely to contain stored electronic communications (including retrieved and un-retrieved
22 email for their subscribers) and information concerning subscribers and their use of the
23
24

1 provider's services, such as account access information, email transaction information,
2 documents, pictures, and account application information.

3 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

4 28. Your Affiant anticipates executing this warrant under the Electronic
5 Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and
6 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies
7 of the records and other information (including the content of communications)
8 particularly described in Section I of Attachment "B." Upon receipt of the information
9 described in Section I of Attachment "B," government-authorized persons will review
10 that information to locate the items described in Section II of Attachment "B."

11 **CONCLUSION**

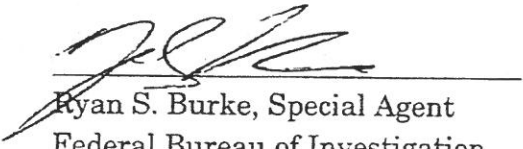
12 29. Based on the forgoing, I request that the Court issue the proposed search
13 warrant. This Court has jurisdiction to issue the requested warrant because it is "a court
14 of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A)
15 & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has
16 jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to
17 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the
18 service or execution of this warrant.

19 **REQUEST FOR SEALING**

20 30. I further request that the Court order that all papers in support of this
21 application, including the affidavit and search warrant, be sealed until further order of
22 the Court. These documents discuss an ongoing criminal investigation that is neither
23 public nor known to all of the targets of the investigation. Accordingly, there is good
24

1 cause to seal these documents because their premature disclosure may seriously
2 jeopardize that investigation.

3
4
5 Respectfully Submitted,

6 
7 Ryan S. Burke, Special Agent
Federal Bureau of Investigation

8
9 SWORN TO AND SUBSCRIBED
before me this 10th day of October 2017.

10
11 
12 UNITED STATES MAGISTRATE JUDGE
13
14
15
16
17
18
19
20
21
22
23
24

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "A"

ONLINE ACCOUNT TO BE SEARCHED

1. This warrant applies to information associated with the Google email account centralpark4804@gmail.com (the "Target Account") from its inception to present, which is stored at premises owned, maintained, controlled, or operated by Google, Inc., headquartered at 1600 Amphitheatre Way, Mountain View, California, 94043.

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from account inception to present:

- a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
- d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
- e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Google-related facility.

1 II. Information to be seized by the United States

2 After reviewing all information described in Section I, the United States will seize
3 evidence of violations of Title 18, United States Code Sections 32(a)
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
5 International Airport); and 922(a)(3); 5 (Unlawful Interstate Transport/Delivery of
6 Firearms by Non Federal Firearms Licensee) (the "Subject Offenses") that occur in the
7 form of the following, from account inception to present:

- 8 a. Communications, transactions and records that may establish ownership
9 and control (or the degree thereof) of the Target Account, including address
10 books, contact or buddy lists, bills, invoices, receipts, registration records,
11 bills, correspondence, notes, records, memoranda, telephone/address books,
12 photographs, video recordings, audio recordings, lists of names, records of
13 payment for access to newsgroups or other online subscription services, and
14 attachments to said communications, transactions and records.
- 15 b. Communications, transactions and records to/from persons who may be co-
16 conspirators of the Subject Offenses, or which may identify co-conspirators.
- 17 c. Communications, transactions and records which may show motivation to
18 commit the Subject Offenses.
- 19 d. Communications, transactions and records that relate to the Subject
20 Offenses.
- 21 e. The terms "communications," "transactions," "records," "documents,"
22 "programs," or "materials" include all information recorded in any form,
23 visual or aural, and by any means, whether in handmade form (including,
24 but not limited to, writings, drawings, paintings), photographic form
25 (including, but not limited to, pictures or videos), or electrical, electronic or
26 magnetic form, as well as digital data files. These terms also include any
27 applications (i.e. software programs). These terms expressly include, among
28 other things, Emails, instant messages, chat logs, correspondence attached
29 as to Emails (or drafts), calendar entries, buddy lists.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "C"

**PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT**

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

1 5. The search procedures utilized for this review are at the sole discretion of
2 the investigating and prosecuting authorities, and may include the following techniques
(the following is a non-exclusive list, as other search procedures may be used):

3 a. examination of all of the data contained in the Search Warrant Data to view
4 the data and determine whether that data falls within the items to be seized as set forth
herein;

5 b. searching for and attempting to recover from the Search Warrant Data any
6 deleted, hidden, or encrypted data to determine whether that data falls within the list
7 of items to be seized as set forth herein (any data that is encrypted and unreadable will
8 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

9 c. surveying various file directories and the individual files they contain;

10 d. opening files in order to determine their contents;

11 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

12 f. scanning storage areas;

13 g. performing keyword searches through all electronic storage areas to
14 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A; and/or

15 h. performing any other data analysis technique that may be necessary to
16 locate and retrieve the evidence described in Attachment B, Section II.

17 **Return and Review Procedures**

18 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

19 (e) Issuing the Warrant.

20 (2) Contents of the Warrant.

21 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
22 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
23 be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
4 copying of electronically stored information. Unless otherwise specified, the warrant
5 authorizes a later review of the media or information consistent with the warrant. The
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
7 on-site copying of the media or information, and not to any later off-site copying or
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare
9 and verify an inventory of any property seized. . . . In a case involving the seizure of
10 electronic storage media or the seizure or copying of electronically stored information,
11 the inventory may be limited to describing the physical storage media that were seized
12 or copied. The officer may retain a copy of the electronically stored information that was
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
15 of the warrant, an agent is required to file an inventory return with the Court, that is,
16 to file an itemized list of the property seized. Execution of the warrant begins when
17 the United States serves the warrant on the named custodian; execution is complete
18 when the custodian provides all Search Warrant Data to the United States. Within
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be
20 filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
19 which the electronically stored information must be seized after the issuance of the
20 warrant and copied after the execution of the warrant, not the "later review of the media
21 or information" seized, or the later off-site digital copying of that media.

22 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
23 may be limited to a description of the "physical storage media" into which the Search
24 Warrant Data that was seized was placed, not an itemization of the information or data
stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
2 purposes of the investigation. The government proposes that the original storage media
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return
5 of any information in the Search Warrant Data that is not set forth in Attachment B,
6 Section II, that information will be copied onto appropriate media and returned to the
7 person from whom the information was seized.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

UNITED STATES DISTRICT COURT

for the
District of NevadaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

CENTRALPARK1@LIVE.COM - A1

Case No. 2:17-mj- 968 - NJK

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

YOU ARE COMMANDED to execute this warrant on or before October 20, 2017 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Nancy J. Koppe
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____Date and time issued: 10/16/2017 4:05pmCity and state: Las Vegas, Nevada

Judge's signature

Printed name and title

1 ATTACHMENT "A1"

2 ONLINE ACCOUNT TO BE SEARCHED

3 1. This warrant applies to information associated with the Microsoft email
4 account centralpark1@live.com (the "Target Accounts") from their inception to present,
5 which is stored at premises owned, maintained, controlled, or operated by Microsoft
6 Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachment A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A1 and A2 from account inception to present:

- a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
- d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
- e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Microsoft-related facility.

II. Information to be seized by the United States

1
2 After reviewing all information described in Section I, the United States will seize
3 evidence of violations of Title 18, United States Code Sections 32(a)
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
5 International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of
6 Firearms by Non Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject
7 Offenses") that occur in the form of the following, from account inception to present:

- 8
9
10 a. Communications, transactions and records that may establish ownership
11 and control (or the degree thereof) of the Target Account, including address
12 books, contact or buddy lists, bills, invoices, receipts, registration records,
13 bills, correspondence, notes, records, memoranda, telephone/address books,
14 photographs, video recordings, audio recordings, lists of names, records of
15 payment for access to newsgroups or other online subscription services, and
16 attachments to said communications, transactions and records.
17 b. Communications, transactions and records to/from persons who may be co-
18 conspirators of the Subject Offenses, or which may identify co-conspirators.
19 c. Communications, transactions and records which may show motivation to
20 commit the Subject Offenses.
21 d. Communications, transactions and records that relate to the Subject
22 Offenses.
23 e. The terms "communications," "transactions," "records," "documents,"
24 "programs," or "materials" include all information recorded in any form,
visual or aural, and by any means, whether in handmade form (including,
but not limited to, writings, drawings, paintings), photographic form
(including, but not limited to, pictures or videos), or electrical, electronic or
magnetic form, as well as digital data files. These terms also include any
applications (i.e. software programs). These terms expressly include, among
other things, Emails, instant messages, chat logs, correspondence attached
as to Emails (or drafts), calendar entries, buddy lists.

ATTACHMENT "C"

1 **PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED**
2 **PURSUANT TO THIS SEARCH WARRANT**

3 1. In executing this warrant, the government must make reasonable efforts to
4 use methods and procedures that will locate and expose in the electronic data produced
5 in response to this search warrant ("the Search Warrant Data") those categories of data,
6 files, documents, or other electronically stored information that are identified with
7 particularity in the warrant, while minimizing exposure or examination of irrelevant,
8 privileged, or confidential files to the extent reasonably practicable.

9 2. When the Search Warrant Data is received, the government will make a
10 duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The
11 original version of the Search Warrant Data will be sealed and preserved for purposes
12 of: later judicial review or order to return or dispose of the Search Warrant Data;
13 production to the defense in any criminal case if authorized by statute, rule, or the
14 Constitution; for purposes of showing the chain of custody of the Search Warrant Data
15 and the Search Warrant Data Copy; or for any other lawful purpose. The original of the
16 Search Warrant Data will not be searched or examined except to ensure that it has been
17 fully and completely replicated in the Search Warrant Data Copy.

18 3. The investigating agents will then search the entirety of the Search
19 Warrant Data Copy using any and all methods and procedures deemed appropriate by
20 the United States designed to identify the information listed as Information to be Seized
21 in Attachment B, Section II. The United States may copy, extract or otherwise segregate
22 information or data listed as Information to be Seized in Attachment B, Section II.
23 Information or data so copied, extracted or otherwise segregated will no longer be subject
24 to any handling restrictions that might be set out in this protocol beyond those required
25 by binding law. To the extent evidence of crimes not within the scope of this warrant
26 appear in plain view during this review, a supplemental or "piggyback" warrant will be
27 applied for in order to further search that document, data, or other item.

28 4. Once the Search Warrant Data Copy has been thoroughly and completely
29 examined for any document, data, or other items identified in Attachment B, Section II
30 as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject
31 to any further search or examination unless authorized by another search warrant or
32 other appropriate court order. The Search Warrant Data Copy will be held and preserved
33 for the same purposes identified above in Paragraph 2.

34 5. The search procedures utilized for this review are at the sole discretion of
35 the investigating and prosecuting authorities, and may include the following techniques
36 (the following is a non-exclusive list, as other search procedures may be used):

1 a. examination of all of the data contained in the Search Warrant Data to view
2 the data and determine whether that data falls within the items to be seized as set forth
herein;

3 b. searching for and attempting to recover from the Search Warrant Data any
4 deleted, hidden, or encrypted data to determine whether that data falls within the list
5 of items to be seized as set forth herein (any data that is encrypted and unreadable will
6 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

7 c. surveying various file directories and the individual files they contain;

8 d. opening files in order to determine their contents;

9 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

10 f. scanning storage areas;

11 g. performing keyword searches through all electronic storage areas to
12 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A1 and A2; and/or

13 h. performing any other data analysis technique that may be necessary to
14 locate and retrieve the evidence described in Attachment B, Section II.

15 **Return and Review Procedures**

16 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

17 (e) Issuing the Warrant.

18 (2) Contents of the Warrant.

19 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
20 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
21 be returned. The warrant must command the officer to:

22 (i) execute the warrant within a specified time no longer than 14 days;

23 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
24

1 copying of electronically stored information. Unless otherwise specified, the warrant
2 authorizes a later review of the media or information consistent with the warrant. The
3 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
on-site copying of the media or information, and not to any later off-site copying or
review.

4 (f) Executing and Returning the Warrant.

5 (1) Warrant to Search for and Seize a Person or Property.

6 (B) Inventory. An officer present during the execution of the warrant must prepare
7 and verify an inventory of any property seized. . . . In a case involving the seizure of
8 electronic storage media or the seizure or copying of electronically stored information,
the inventory may be limited to describing the physical storage media that were seized
9 or copied. The officer may retain a copy of the electronically stored information that was
seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in
accordance with the following:

11 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
12 of the warrant, an agent is required to file an inventory return with the Court, that is,
to file an itemized list of the property seized. Execution of the warrant begins when
13 the United States serves the warrant on the named custodian; execution is complete
when the custodian provides all Search Warrant Data to the United States. Within
14 fourteen (14) days of completion of the execution of the warrant, the inventory will be
15 filed.

16 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
which the electronically stored information must be seized after the issuance of the
17 warrant and copied after the execution of the warrant, not the "later review of the media
or information" seized, or the later off-site digital copying of that media.

18 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
19 may be limited to a description of the "physical storage media" into which the Search
Warrant Data that was seized was placed, not an itemization of the information or data
20 stored on the "physical storage media" into which the Search Warrant Data was placed;

21 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
22 purposes of the investigation. The government proposes that the original storage media
on which the Search Warrant Data was placed plus a full image copy of the seized Search
23 Warrant Data be retained by the government.

1 e. If the person from whom any Search Warrant Data was seized requests the return
2 of any information in the Search Warrant Data that is not set forth in Attachment B,
3 Section II, that information will be copied onto appropriate media and returned to the
4 person from whom the information was seized.
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

1 STEVEN W. MYHRE
Acting United States Attorney
2 District of Nevada
CRISTINA D. SILVA
3 PATRICK BURNS
Assistant United States Attorneys
4 501 Las Vegas Blvd. South, Ste. 1100
Las Vegas, Nevada 89101
Telephone: (702) 388-6336
5 Fax (702) 388-6698
john.p.burns@usdoj.gov

6 Attorney for the United States of America
7

8 **UNITED STATES DISTRICT COURT**
9 **DISTRICT OF NEVADA**

-oOo-

10 IN THE MATTER OF THE SEARCH OF
11 INFORMATION ASSOCIATED WITH
EMAIL ACCOUNTS
12 CENTRALPARK1@LIVE.COM THAT IS
STORED AT A PREMISES
13 CONTROLLED BY MICROSOFT. A1

Magistrate No. 17-mj-968-NJK

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH
WARRANTS**

(Under Seal)

14 IN THE MATTER OF THE SEARCH OF
15 INFORMATION ASSOCIATED WITH
EMAIL ACCOUNTS
16 MARILOUROSES@LIVE.COM THAT IS
STORED AT A PREMISES
17 CONTROLLED BY MICROSOFT. A2

Magistrate No.

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH
WARRANTS**

(Under Seal)

18
19
20
21 STATE OF NEVADA)
22) ss:
23 COUNTY OF CLARK)
24

1 **AFFIDAVIT IN SUPPORT OF AN**
2 **APPLICATION FOR SEARCH WARRANTS**

3 I, Ryan S. Burke, Special Agent, Federal Bureau of Investigation (FBI), having
4 been duly sworn, hereby depose and say:

5 **INTRODUCTION AND AGENT BACKGROUND**

6 1. Your Affiant makes this affidavit in support of an application for search
7 warrants for information associated with email accounts centralpark1@live.com ("Target
8 Account 1") and marilouroses@live.com ("Target Account 2"). Target Account 1 is an
9 account associated with STEPHEN PADDOCK. Target Account 2 is an account
10 associated with MARILOU DANLEY. The information associated with both accounts is
11 stored at a premises owned, maintained, controlled, or operated by Microsoft
12 Corporation ("Microsoft"), an American multinational technology company based in
13 Redmond, Washington that specializes in Internet-related services and products along
14 with the development and manufacturing of computer-related items. Those online
15 services include, but are not limited to, email services, cloud computing, and many other
16 services. The information to be searched is described in the following paragraphs and in
17 Attachment "A" (attached hereto and incorporated herein by reference). This affidavit is
18 made in support of an application for search warrants under 18 U.S.C. §§ 2703(a),
19 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft to disclose to the government
20 records and other information in its possession, pertaining to the subscriber or customer
21 associated with the Target Accounts.

22 2. I am an "investigative or law enforcement officer of the United States"
23 within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of
24

1 the United States who is empowered by law to conduct investigations of, and to make
2 arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

3 3. I have been employed as a Special Agent of the FBI for approximately five
4 years, which began at the FBI Academy in October 2012. Upon completion of the
5 academy, I was transferred to the Las Vegas Division's white collar crime squad and
6 then the human trafficking squad. Since October 2015, I have been assigned to the Las
7 Vegas Division's violent crime/gang squad. Additionally, I have been a certified member
8 of the FBI's Cellular Analysis Survey Team since August 2015 due to my expertise in
9 the field of historical cell site analysis.

10 4. During my tenure with the FBI, I have conducted surveillance, analyzed
11 telephone records, interviewed witnesses, supervised activities of sources, executed
12 search warrants, executed arrest warrants, and participated in court-authorized
13 interceptions of wire and electronic communications. These investigative activities have
14 been conducted in conjunction with a variety of investigations, to include those involving
15 robbery, drug trafficking, kidnapping, murder, criminal enterprises, and more. In
16 addition to my practical experiences, I received five months of extensive law enforcement
17 training at the FBI Academy.

18 5. The facts in this affidavit are derived from your Affiant's personal
19 observations, his training and experience, and information obtained from other agents,
20 detectives, and witnesses. This affidavit is intended to show merely that there is
21 sufficient probable cause for the requested warrants and does not set forth all of the
22 Affiant's knowledge about this matter.
23
24

1 6. Based on your Affiant's training and experience and the facts as set forth
2 in this affidavit, there is probable cause to believe that violations of:

- 3 a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C.A. § 32(a);
4 b. Violence at International Airport - 18 U.S.C. § 37(a)(2); and
5 c. Unlawful Interstate Transport/Delivery of Firearms by Non Federal
6 Firearms Licensee - 18 U.S.C. §§ 922(a)(3) and (5);
7 d. Aiding and Abetting - 18 U.S.C. § 2.

8 (hereafter, "Subject Offenses") have been committed by STEPHEN PADDOCK,
9 MARILOU DANLEY, and others yet unknown. There is also probable cause to search
10 the information described in Attachment "A" for evidence of these crimes and
11 information which might reveal the identities of others involved in these crimes, as
12 described in Attachment "B" (attached hereto and incorporated herein by reference).

13 **PROBABLE CAUSE**

14 7. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music
15 festival, was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At
16 approximately 10:08 p.m., the Las Vegas Metropolitan Police Department (LVMPD)
17 received calls reporting shots had been fired at the concert and multiple victims were
18 struck. LVMPD determined the shots were coming from Rooms 134 and 135 on the 32nd
19 floor of the Mandalay Bay Resort and Casino, located due west of the festival rounds at
20 3950 South Las Vegas Boulevard, Las Vegas, Nevada. These rooms are an elevated
21 position which overlooks the concert venue. Witness statements and video
22 footage captured during the attack indicates that the weapons being used were firing in
23 a fully-automatic fashion.
24

1 8. LVMPD officers ultimately made entry into the room and located an
2 individual later identified as Stephen Paddock. Paddock was deceased from an apparent
3 self-inflicted gunshot wound.

4 9. Paddock's Nevada driver's license was located in the Mandalay Bay hotel
5 room with Paddock, and both hotel rooms were registered in his name. A player's club
6 card in name of Marilou Danley was located in Paddock's room, and the card returned
7 to the address located on Babbling Brook Street in Mesquite, Nevada. FBI Agents
8 located Danley, who was traveling outside the United States at the time of the
9 shooting. It was ultimately determined that Danley resided with Paddock at the
10 Babbling Brook address.

11 10. On October 2, 2017, search warrants were executed on Paddock's Mandalay
12 Bay hotel rooms, Paddock's vehicle at Mandalay Bay, and two Nevada residences owed
13 by Paddock: 1372 Babbling Brook Court in Mesquite, and 1735 Del Webb Parkway in
14 Reno, Nevada. Officers and Agents found over 20 firearms, hundreds of rounds of
15 ammunition, and hundreds of spent shell casings in the Mandalay Bay hotel rooms, in
16 close proximity to Paddock's body. Over a thousand rounds of rifle ammunition and 100
17 pounds of explosive material was found in Paddock's vehicle. Additional explosive
18 material, approximately 18 firearms, and over 1,000 rounds of ammunition was located
19 at the Mesquite residence. A large quantity of ammunition and multiple firearms were
20 recovered from the Reno residence.

21 11. As of this date, 58 people have been identified to have been killed in
22 Paddock's attack and another 557 were reportedly injured. Additionally, investigators
23 discovered that STEPHEN PADDOCK also utilized a firearm to shoot large fuel tanks
24

1 on Las Vegas McCarran International Airport property. Multiple bullet holes were found
2 on the tank, which investigators believe was an attempt by STEPHEN PADDOCK to
3 cause the tanks to explode.

4 12. In an effort to determine whether or not STEPHEN PADDOCK was
5 assisted and/or conspired with unknown individuals, investigators have attempted to
6 identify all of STEPHEN PADDOCK's associated. It was quickly determined that a
7 casino player's card in the name of MARILOU DANLEY was located in the room at the
8 time of the attack. She has been identified thus far as the most likely person who aided
9 or abetted STEPHEN PADDOCK based on her informing law enforcement that her
10 fingerprints would likely be found on the ammunition used during the attack.
11 Subsequently, investigators worked to identify the communication facilities utilized by
12 STEPHEN PADDOCK and MARILOU DANLEY.

13 13. Based on a review of STEPHEN PADDOCK's financial accounts, Target
14 Account 1 was determined to belong to STEPHEN PADDOCK. On October 3, 2017,
15 investigators requested an emergency disclosure of records from Microsoft related to
16 Target Account 1 so it could be immediately searched for any evidence of additional co-
17 conspirators. Unfortunately, the information was only requested for a six month
18 timeframe. Within the account, investigators identified Target Account 2 as one that
19 belonged to MARILOU DANLEY, which was clear based on the communications
20 between the two email accounts.

21 14. On September 25, 2017, an email was exchanged between the Target
22 Accounts which discussed a wire transfer of funds which was to be sent by STEPHEN
23
24

1 PADDOCK to MARILOU DANLEY. It is unclear what the purpose of the wire transfer
2 was, but MARILOU DANLEY is known to have been in the Philippines at the time.

3 15. Additionally, on July 6, 2017, Target Account 1 sent an email to
4 centralpark4804@gmail.com which read, "try an ar before u buy. we have huge selection.
5 located in the las vegas area." Later that day, an email was received back from
6 centralpark4804@gmail.com to Target Account 1 that read, "we have a wide variety of
7 optics and ammunition to try." And lastly, Target Account 1 later sent an email to
8 centralpark4804@gmail.com that read, "for a thrill try out bumpfire ar's with a 100
9 round magazine." Investigators believe these communications may have been related to
10 the eventual attack that occurred at the Mandalay Bay in Las Vegas.

11 16. Your Affiant believes the requested search warrants will yield significant
12 information from Microsoft such as STEPHEN PADDOCK's and MARILOU DANLEY's
13 contact lists, email messages content, IP address usage, photographs, third-party
14 applications associated with the account, and more, which may constitute evidence of
15 the planning of the attack and potentially identify other participants in the attack.
16 Ultimately, your Affiant strongly believes the requested information will lead
17 investigators to determine the full scope of STEPHEN PADDOCK's plan and MARILOU
18 DANLEY's possible involvement.

19 RELEVANT TECHNICAL TERMS

20 17. The following non-exhaustive list of definitions applies to this Affidavit and
21 the Attachments to this Affidavit:

22 a. The "Internet" is a worldwide network of computer systems operated
23 by governmental entities, corporations, and universities. In order to access the Internet,
24

1 an individual computer user must subscribe to an access provider, which operates a host
2 computer system with direct access to the Internet. The World Wide Web is a
3 functionality of the Internet which allows users of the Internet to share information.

4 b. "Internet Service Providers" are companies that provide access to the
5 Internet. ISPs can also provide other services for their customers including website
6 hosting, email service, remote storage, and co-location of computers and other
7 communications equipment. ISPs offer different ways to access the Internet including
8 telephone-based (dial-up), broadband-based access via a digital subscriber line (DSL) or
9 cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge
10 a fee based upon the type of connection and volume of data (bandwidth). Many ISPs
11 assign each subscriber an account name, such as a user name, an email address, and an
12 email mailbox, and the subscriber typically creates a password for his/her account.

13 c. "ISP Records" are records maintained by ISPs pertaining to their
14 subscribers (regardless of whether those subscribers are individuals or entities). These
15 records may include account application information, subscriber and billing information,
16 account access information (often in the form of log files), emails, information concerning
17 content uploaded and/or stored on the ISP's servers, and other information, which may
18 be stored both in computer data format and in written or printed record format. ISPs
19 reserve and/or maintain computer disk storage space on their computer system for their
20 subscribers' use. This service by ISPs allows for both temporary and long-term storage
21 of electronic communications and many other types of electronic data and files.

22 d. "Online service providers" (also referred to here as "service
23 providers") are companies that provide online services such as email, chat or instant
24

1 messaging, word processing applications, spreadsheet applications, presentation
2 applications similar to PowerPoint, online calendar, photo storage and remote storage
3 services. Sometimes they also can provide web hosting, remote storage, and co-location
4 of computers and other communications equipment. Typically, each service provider
5 assigns each subscriber an account name, such as a user name or screen name and the
6 subscriber typically creates a password for his/her account.

7 e. "Computer," as used herein, is defined as "an electronic, magnetic,
8 optical, electrochemical, or other high speed data processing device performing logical or
9 storage functions, and includes any data storage facility or communications facility
10 directly related to or operating in conjunction with such device."

11 f. A "server" is a centralized computer that provides services for other
12 computers connected to it via a network. The other computers attached to a server are
13 sometimes called "clients." For example, in a large company, it is common for individual
14 employees to have client computers at their desktops. When the employees access their
15 email, or access files stored on the network itself, those files are pulled electronically
16 from the server, where they are stored, and are sent to the client's computer via the
17 network. Notably, servers can be physically stored in any location: it is not uncommon
18 for a network's server to be located hundreds (and even thousands) of miles away from
19 the client computers.

20 g. "Internet Protocol address," or "IP address," refers to a unique
21 number used by a computer to access the Internet. IP addresses can be dynamic,
22 meaning that the Internet Service Provider (ISP) assigns a different unique number to
23 a computer every time it accesses the Internet. IP addresses might also be static, that
24

1 is, an ISP assigns a user's computer a particular IP address which is used each time the
2 computer accesses the Internet.

3 h. The term "domain" refers to a word used as a name for computers,
4 networks, services, etc. A domain name typically represents a website, a server computer
5 that hosts that website, or even some computer (or other digital device) connected to the
6 internet. Essentially, when a website (or a server computer that hosts that website) is
7 connected to the internet, it is assigned an IP address. Because IP addresses are difficult
8 for people to remember, domain names are instead used because they are easier to
9 remember than IP addresses. Domain names are formed by the rules and procedures of
10 the Domain Name System (DNS). A common top level domain under these rules is ".com"
11 for commercial organizations, ".gov" for the United States government, and ".org" for
12 organizations. For example, www.usdoj.gov is the domain name that identifies a server
13 used by the U.S. Department of Justice, and which uses IP address of 149.101.46.71.

14 i. "Web hosting services" maintain server computers connected to the
15 Internet. Their customers use those computers to operate websites on the Internet.
16 Customers of web hosting companies place files, software code, databases, and other data
17 on servers. To do this, customers typically connect from their own computers to the
18 server computers across the Internet.

19 j. The term "WhoIs" lookup refers to a search of a publicly available
20 online database that lists information provided when a domain is registered or when an
21 IP address is assigned.

22 k. The terms "communications," "records," "documents," "programs," or
23 "materials" include all information recorded in any form, visual or aural, and by any
24

1 means, whether in handmade form (including, but not limited to, writings, drawings,
2 paintings), photographic form (including, but not limited to, pictures or videos), or
3 electrical, electronic or magnetic form, as well as digital data files. These terms also
4 include any applications (i.e. software programs). These terms expressly include, among
5 other things, emails, instant messages, chat logs, correspondence attached as to emails
6 (or drafts), calendar entries, buddy lists.

7 1. "Chat" is usually a real time electronic communication between two
8 or more individuals. Unlike email, which is frequently sent, then read and responded to
9 minutes, hours, or even days later, chats frequently involve an immediate conversation
10 between individuals, similar to a face-to-face conversation. Nearly all chat programs are
11 capable of saving the chat transcript, to enable users to preserve a record of the
12 conversation. By default, some chat programs have this capability enabled, while others
13 do not. Many popular web-based email providers, like Microsoft and Microsoft, provide
14 chat functionality as part of the online services they provide to account holders.

15 **FACTS ABOUT EMAIL PROVIDERS**

16 18. In my training, my experience and this investigation, I have learned that
17 Microsoft (the Service Provider) is a company that provides free web-based Internet
18 email access to the general public, and that stored electronic communications, including
19 opened and unopened email for Microsoft subscribers may be located on the computers
20 of Microsoft. I have also learned that Microsoft Inc. provides various on-line service
21 messaging services to the general public. Instant Messaging ("IM") is a form of real-time
22 direct text-based communication between two or more people using shared clients. The
23 text is conveyed via devices connected over a network such as the Internet. In addition
24

1 to text, Microsoft's software allows users with the most current updated versions to
2 utilize its webcam service. This option enables users from distances all over the world to
3 view others who have installed a webcam on their end. Thus, the Service Provider's
4 servers will contain a wide variety of the subscriber's files, including emails, address
5 books, contact or buddy lists, calendar data, pictures, chat logs, and other files.

6 19. To use these services, subscribers register for online accounts like the
7 Target Accounts. During the registration process, service providers such as the ones here
8 ask subscribers to provide basic personal information. This information can include the
9 subscriber's full name, physical address, telephone numbers and other identifiers,
10 alternative email addresses, and, for paying subscribers, means and source of payment
11 (including any credit card or bank account number). Based on my training and my
12 experience, I know that subscribers may insert false information to conceal their
13 identity; even if this proves to be the case, however, I know that this information often
14 provide clues to their identity, location or illicit activities.

15 20. In general, when a subscriber receives an email, it is typically stored in the
16 subscriber's "mail box" on that service provider's servers until the subscriber deletes the
17 Email. If the subscriber does not delete the message, the message (and any attachments)
18 can remain on that service provider's servers indefinitely.

19 21. Similarly, when the subscriber sends an email, it is initiated at the
20 subscriber's computer, transferred via the Internet to the service provider's servers, and
21 then transmitted to its end destination. That service provider often saves a copy of the
22 email sent. Unless the sender of the email specifically deletes the Email from the
23 provider's server, the email can remain on the system indefinitely.

1 22. A sent or received email typically includes the content of the message,
2 source and destination addresses, the date and time at which the email was sent, and
3 the size and length of the email. If an email user writes a draft message but does not
4 send it, that message may also be saved by that service provider, but may not include all
5 of these categories of data.

6 23. Just as a computer on a desk can be used to store a wide variety of files, so
7 can online accounts, such as the accounts subject to this application. First, subscribers
8 can store many types of files as attachments to emails in online accounts. Second,
9 because service providers provide the services listed above (e.g. word processing,
10 spreadsheets, pictures), subscribers who use these services usually store documents on
11 servers maintained and/or owned by service providers. Thus, these online accounts often
12 contain documents such as pictures, audio or video recordings, logs, spreadsheets,
13 applications and other files.

14 24. Reviewing files stored in online accounts raises many of the same
15 difficulties as with reviewing files stored on a local computer. For example, based on my
16 training, my experience and this investigation, I know that subscribers of these online
17 services can conceal their activities by altering files before they upload them to the online
18 service. Subscribers can change file names to more innocuous sounding names (e.g.
19 renaming "FraudRecords.doc" to "ChristmasList.doc"), they can change file extensions
20 to make one kind of file appear like a different type of file (e.g. changing the spreadsheet
21 "StolenCreditProfiles.xls" to "FamilyPhoto.jpg" to appear to be a picture file, where the
22 file extension ".xls" denotes an Excel spreadsheet file and ".jpg" a JPEG format image
23 file), or they can change the times and dates a file was last accessed or modified by
24

1 changing a computer's system time/date and then uploading that file to the Online
2 Accounts. Thus, to detect any files that the subscriber may have concealed, agents will
3 need to review all of the files in the Target Accounts; they will, however, only seize the
4 items that the Court authorizes to be seized. Similarly, subscribers can conceal their
5 activities by encrypting files. Thus, these files may need to be decrypted to detect
6 whether it constitutes an Item to be Seized.

7 25. I also believe that people engaged in crimes such as the one described
8 herein often use online accounts because they give people engaged in these crimes a way
9 to easily communicate with other co-conspirators. Moreover, online accounts are easily
10 concealed from law enforcement. Unlike physical documents, electronic documents can
11 be stored in a physical place far away, where they are less likely to be discovered.

12 26. Service providers typically retain certain transactional information about
13 the creation and use of each account on their systems. This information can include the
14 date on which the account was created, the length of service, records of log-in (i.e.,
15 session) times and durations, the types of service utilized, the status of the account
16 (including whether the account is inactive or closed), the methods used to connect to the
17 account (such as logging into the account via websites controlled by the Service
18 Provider), and other log files that reflect usage of the account. In addition, service
19 providers often have records of the Internet Protocol address ("IP address") used to
20 register the account and the IP addresses associated with particular logins to the
21 account. Because every device that connects to the Internet must use an IP address, IP
22 address information can help to identify which computers or other devices were used to
23 access the online account.

1 27. In some cases, subscribers will communicate directly with a service
2 provider about issues relating to the account, such as technical problems, billing
3 inquiries, or complaints from or about other users. Service providers typically retain
4 records about such communications, including records of contacts between the user and
5 the provider's support services, as well records of any actions taken by the provider or
6 user as a result of the communications.

7 28. In my training and experience, evidence of who was using an online
8 account may be found in address books, contact or buddy lists, emails in the account,
9 and pictures and files, whether stored as attachments or in the suite of the service
10 provider's online applications. Therefore, the computers of the Service Providers are
11 likely to contain stored electronic communications (including retrieved and un-retrieved
12 email for their subscribers) and information concerning subscribers and their use of the
13 provider's services, such as account access information, email transaction information,
14 documents, pictures, and account application information.

15 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

16 29. Your Affiant anticipates executing these warrants under the Electronic
17 Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and
18 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government
19 copies of the records and other information (including the content of communications)
20 particularly described in Section I of Attachment "B." Upon receipt of the information
21 described in Section I of Attachment "B," government-authorized persons will review
22 that information to locate the items described in Section II of Attachment "B."

23 **CONCLUSION**

30. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

31. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully Submitted,

Ryan S. Burke, Special Agent
Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED
before me this 6th day of October 2017.

UNITED STATES MAGISTRATE JUDGE

1 ATTACHMENT "A1"

2 ONLINE ACCOUNT TO BE SEARCHED

3 1. This warrant applies to information associated with the Microsoft email
4 account centralpark1@live.com (the "Target Accounts") from their inception to present,
5 which is stored at premises owned, maintained, controlled, or operated by Microsoft
6 Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

1 ATTACHMENT "A2"

2 ONLINE ACCOUNT TO BE SEARCHED

3 1. This warrant applies to information associated with the Microsoft email
4 account marilouroses@live.com (the "Target Accounts") from their inception to present,
5 which is stored at premises owned, maintained, controlled, or operated by Microsoft
6 Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachment A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A1 and A2 from account inception to present:

- a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
- d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
- e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Microsoft-related facility.

II. Information to be seized by the United States

1
2 After reviewing all information described in Section I, the United States will seize
3 evidence of violations of Title 18, United States Code Sections 32(a)
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
5 International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of
6 Firearms by Non Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject
7 Offenses") that occur in the form of the following, from account inception to present:

- 8
9
10 a. Communications, transactions and records that may establish ownership
11 and control (or the degree thereof) of the Target Account, including address
12 books, contact or buddy lists, bills, invoices, receipts, registration records,
13 bills, correspondence, notes, records, memoranda, telephone/address books,
14 photographs, video recordings, audio recordings, lists of names, records of
15 payment for access to newsgroups or other online subscription services, and
16 attachments to said communications, transactions and records.
17 b. Communications, transactions and records to/from persons who may be co-
18 conspirators of the Subject Offenses, or which may identify co-conspirators.
19 c. Communications, transactions and records which may show motivation to
20 commit the Subject Offenses.
21 d. Communications, transactions and records that relate to the Subject
22 Offenses.
23 e. The terms "communications," "transactions," "records," "documents,"
24 "programs," or "materials" include all information recorded in any form,
visual or aural, and by any means, whether in handmade form (including,
but not limited to, writings, drawings, paintings), photographic form
(including, but not limited to, pictures or videos), or electrical, electronic or
magnetic form, as well as digital data files. These terms also include any
applications (i.e. software programs). These terms expressly include, among
other things, Emails, instant messages, chat logs, correspondence attached
as to Emails (or drafts), calendar entries, buddy lists.

ATTACHMENT "C"

1 **PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED**
2 **PURSUANT TO THIS SEARCH WARRANT**

3 1. In executing this warrant, the government must make reasonable efforts to
4 use methods and procedures that will locate and expose in the electronic data produced
5 in response to this search warrant ("the Search Warrant Data") those categories of data,
6 files, documents, or other electronically stored information that are identified with
7 particularity in the warrant, while minimizing exposure or examination of irrelevant,
8 privileged, or confidential files to the extent reasonably practicable.

9 2. When the Search Warrant Data is received, the government will make a
10 duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The
11 original version of the Search Warrant Data will be sealed and preserved for purposes
12 of: later judicial review or order to return or dispose of the Search Warrant Data;
13 production to the defense in any criminal case if authorized by statute, rule, or the
14 Constitution; for purposes of showing the chain of custody of the Search Warrant Data
15 and the Search Warrant Data Copy; or for any other lawful purpose. The original of the
16 Search Warrant Data will not be searched or examined except to ensure that it has been
17 fully and completely replicated in the Search Warrant Data Copy.

18 3. The investigating agents will then search the entirety of the Search
19 Warrant Data Copy using any and all methods and procedures deemed appropriate by
20 the United States designed to identify the information listed as Information to be Seized
21 in Attachment B, Section II. The United States may copy, extract or otherwise segregate
22 information or data listed as Information to be Seized in Attachment B, Section II.
23 Information or data so copied, extracted or otherwise segregated will no longer be subject
24 to any handling restrictions that might be set out in this protocol beyond those required
25 by binding law. To the extent evidence of crimes not within the scope of this warrant
26 appear in plain view during this review, a supplemental or "piggyback" warrant will be
27 applied for in order to further search that document, data, or other item.

28 4. Once the Search Warrant Data Copy has been thoroughly and completely
29 examined for any document, data, or other items identified in Attachment B, Section II
30 as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject
31 to any further search or examination unless authorized by another search warrant or
32 other appropriate court order. The Search Warrant Data Copy will be held and preserved
33 for the same purposes identified above in Paragraph 2.

34 5. The search procedures utilized for this review are at the sole discretion of
35 the investigating and prosecuting authorities, and may include the following techniques
36 (the following is a non-exclusive list, as other search procedures may be used):

1 a. examination of all of the data contained in the Search Warrant Data to view
2 the data and determine whether that data falls within the items to be seized as set forth
herein;

3 b. searching for and attempting to recover from the Search Warrant Data any
4 deleted, hidden, or encrypted data to determine whether that data falls within the list
5 of items to be seized as set forth herein (any data that is encrypted and unreadable will
6 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

7 c. surveying various file directories and the individual files they contain;

8 d. opening files in order to determine their contents;

9 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

10 f. scanning storage areas;

11 g. performing keyword searches through all electronic storage areas to
12 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A1 and A2; and/or

13 h. performing any other data analysis technique that may be necessary to
14 locate and retrieve the evidence described in Attachment B, Section II.

15 **Return and Review Procedures**

16 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

17 (e) Issuing the Warrant.

18 (2) Contents of the Warrant.

19 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
20 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
21 be returned. The warrant must command the officer to:

22 (i) execute the warrant within a specified time no longer than 14 days;

23 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
24

1 copying of electronically stored information. Unless otherwise specified, the warrant
2 authorizes a later review of the media or information consistent with the warrant. The
3 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
on-site copying of the media or information, and not to any later off-site copying or
review.

4 (f) Executing and Returning the Warrant.

5 (1) Warrant to Search for and Seize a Person or Property.

6 (B) Inventory. An officer present during the execution of the warrant must prepare
7 and verify an inventory of any property seized. . . . In a case involving the seizure of
8 electronic storage media or the seizure or copying of electronically stored information,
the inventory may be limited to describing the physical storage media that were seized
9 or copied. The officer may retain a copy of the electronically stored information that was
seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in
11 accordance with the following:

12 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
13 of the warrant, an agent is required to file an inventory return with the Court, that is,
to file an itemized list of the property seized. Execution of the warrant begins when
14 the United States serves the warrant on the named custodian; execution is complete
when the custodian provides all Search Warrant Data to the United States. Within
15 fourteen (14) days of completion of the execution of the warrant, the inventory will be
filed.

16 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
17 which the electronically stored information must be seized after the issuance of the
warrant and copied after the execution of the warrant, not the "later review of the media
18 or information" seized, or the later off-site digital copying of that media.

19 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
may be limited to a description of the "physical storage media" into which the Search
20 Warrant Data that was seized was placed, not an itemization of the information or data
stored on the "physical storage media" into which the Search Warrant Data was placed;

21 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
22 purposes of the investigation. The government proposes that the original storage media
on which the Search Warrant Data was placed plus a full image copy of the seized Search
23 Warrant Data be retained by the government.

1 e. If the person from whom any Search Warrant Data was seized requests the return
2 of any information in the Search Warrant Data that is not set forth in Attachment B,
3 Section II, that information will be copied onto appropriate media and returned to the
4 person from whom the information was seized.
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

UNITED STATES DISTRICT COURT

for the
District of Nevada

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

ACCOUNT(S) ASSOCIATED WITH THE CELLULAR
DEVICE BEARING IMEI 990006880858377 STORED
AT A PREMISES CONTROLLED BY GOOGLE

Case No. 2:17-mj- 971-NJK

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Nevada
(Identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (Identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

YOU ARE COMMANDED to execute this warrant on or before October 20, 2017 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Henry J. Koppe
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 10/16/2017 8:45 pm

City and state: Las Vegas, Nevada

Judge's signature

Printed name and title

Henry J. Koppe US Magistrate Judge

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "A"

ONLINE ACCOUNT TO BE SEARCHED

1. This warrant applies to information related to the Google account associated with the cellular device bearing IMEI 990006880858377 (the "Target Account") from its inception to present, which is stored at premises owned, maintained, controlled, or operated by Google, Inc., headquartered at 1600 Amphitheatre Way, Mountain View, California, 94043.

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from account inception to present:

- a. The contents of all messages and emails associated with the account, including copies of messages and emails sent to and from the account, draft messages/emails, the source and destination addresses associated with each message/email, the date and time at which each message/email was sent, and the size and length of each message/email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
- d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
- e. All data and contents related to the following Google Services associated with the Target Account: Android; Gmail; Google Calendar; Google Docs; Google Drive; Google Talk; Multilogin; Web History; YouTube; and all other applications.
- f. All information and content associated with any third-party application associated with the Target Account and the dates when the applications were installed;

- 1 g. Based on an analysis of cookies assigned to computers and devices that
2 accessed the Target Account, identify all other Google accounts that have
3 been accessed from any computers and devices that have logged into the
4 Target Account.

5 II. Information to be seized by the United States

6 After reviewing all information described in Section I, the United States will seize
7 evidence of violations of Title 18, United States Code Sections 32(a)
8 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
9 International Airport); and 922(a)(3); 5 (Unlawful Interstate Transport/Delivery of
10 Firearms by Non Federal Firearms Licensee) (the "Subject Offenses") that occur in the
11 form of the following, from account inception to present:

- 12 a. Communications, transactions and records that may establish ownership
13 and control (or the degree thereof) of the Target Account, including address
14 books, contact or buddy lists, bills, invoices, receipts, registration records,
15 bills, correspondence, notes, records, memoranda, telephone/address books,
16 photographs, video recordings, audio recordings, lists of names, records of
17 payment for access to newsgroups or other online subscription services, and
18 attachments to said communications, transactions and records.
- 19 b. Communications, transactions and records to/from persons who may be co-
20 conspirators of the Subject Offenses, or which may identify co-conspirators.
- 21 c. Communications, transactions and records which may show motivation to
22 commit the Subject Offenses.
- 23 d. Communications, transactions and records that relate to the Subject
24 Offenses.
- 25 e. The terms "communications," "transactions," "records," "documents,"
26 "programs," or "materials" include all information recorded in any form,
27 visual or aural, and by any means, whether in handmade form (including,
28 but not limited to, writings, drawings, paintings), photographic form
29 (including, but not limited to, pictures or videos), or electrical, electronic or
30 magnetic form, as well as digital data files. These terms also include any
31 applications (i.e. software programs). These terms expressly include, among
32 other things, Emails, instant messages, chat logs, correspondence attached
33 as to Emails (or drafts), calendar entries, buddy lists.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "C"

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

1 5. The search procedures utilized for this review are at the sole discretion of
2 the investigating and prosecuting authorities, and may include the following techniques
(the following is a non-exclusive list, as other search procedures may be used):

3 a. examination of all of the data contained in the Search Warrant Data to view
4 the data and determine whether that data falls within the items to be seized as set forth
herein;

5 b. searching for and attempting to recover from the Search Warrant Data any
6 deleted, hidden, or encrypted data to determine whether that data falls within the list
7 of items to be seized as set forth herein (any data that is encrypted and unreadable will
8 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

9 c. surveying various file directories and the individual files they contain;

10 d. opening files in order to determine their contents;

11 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

12 f. scanning storage areas;

13 g. performing keyword searches through all electronic storage areas to
14 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A; and/or

15 h. performing any other data analysis technique that may be necessary to
16 locate and retrieve the evidence described in Attachment B, Section II.

17 **Return and Review Procedures**

18 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

19 (e) Issuing the Warrant.

20 (2) Contents of the Warrant.

21 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
22 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
23 be returned. The warrant must command the officer to:
24

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
4 copying of electronically stored information. Unless otherwise specified, the warrant
5 authorizes a later review of the media or information consistent with the warrant. The
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
7 on-site copying of the media or information, and not to any later off-site copying or
8 review.

9 (f) Executing and Returning the Warrant.

10 (1) Warrant to Search for and Seize a Person or Property.

11 (B) Inventory. An officer present during the execution of the warrant must prepare
12 and verify an inventory of any property seized. . . . In a case involving the seizure of
13 electronic storage media or the seizure or copying of electronically stored information,
14 the inventory may be limited to describing the physical storage media that were seized
15 or copied. The officer may retain a copy of the electronically stored information that was
16 seized or copied.

17 7. Pursuant to this Rule, the government understands and will act in
18 accordance with the following:

19 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
20 of the warrant, an agent is required to file an inventory return with the Court, that is,
21 to file an itemized list of the property seized. Execution of the warrant begins when
22 the United States serves the warrant on the named custodian; execution is complete
23 when the custodian provides all Search Warrant Data to the United States. Within
24 fourteen (14) days of completion of the execution of the warrant, the inventory will be
filed.

b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
which the electronically stored information must be seized after the issuance of the
warrant and copied after the execution of the warrant, not the "later review of the media
or information" seized, or the later off-site digital copying of that media.

c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
may be limited to a description of the "physical storage media" into which the Search
Warrant Data that was seized was placed, not an itemization of the information or data
stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
2 purposes of the investigation. The government proposes that the original storage media
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return
5 of any information in the Search Warrant Data that is not set forth in Attachment B,
6 Section II, that information will be copied onto appropriate media and returned to the
7 person from whom the information was seized.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

1 STEVEN W. MYHRE
Acting United States Attorney
2 District of Nevada
CRISTINA D. SILVA
3 PATRICK BURNS
Assistant United States Attorneys
501 Las Vegas Blvd. South, Ste. 1100
4 Las Vegas, Nevada 89101
Telephone: (702) 388-6336
5 Fax (702) 388-6698
john.p.burns@usdoj.gov

6 Attorney for the United States of America

7
8 **UNITED STATES DISTRICT COURT**
DISTRICT OF NEVADA

9 -oOo-

10 IN THE MATTER OF THE SEARCH OF
INFORMATION RELATED TO THE
11 ACCOUNT(S) ASSOCIATED WITH THE
CELLULAR DEVICE BEARING IMEI
12 990006880858377 THAT IS STORED AT
A PREMISES CONTROLLED BY
13 GOOGLE.

Magistrate No. 17-mj-971-NJK

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH
WARRANT**

(Under Seal)

14 STATE OF NEVADA)
15) ss:
COUNTY OF CLARK)

16 **AFFIDAVIT IN SUPPORT OF AN**
17 **APPLICATION FOR A SEARCH WARRANT**

18 I, Ryan S. Burke, Special Agent, Federal Bureau of Investigation (FBI), having
19 been duly sworn, hereby depose and say:

20 **INTRODUCTION AND AGENT BACKGROUND**

21 1. Your Affiant makes this affidavit in support of an application for a search
22 warrant for information related to the Google account(s) associated with the cellular
23 device bearing IMEI 990006880858377 ["Target Account(s)"], which are associated with
24

1 STEPHEN PADDOCK. This information is stored at a premises owned, maintained,
2 controlled, or operated by Google, Inc. ("Google"), an American multinational technology
3 based in Mountain View, California that specializes in Internet-related services and
4 products. Those services include, but are not limited to, online advertising technologies,
5 a search engine, email services, cloud computing, and many other services. The
6 information to be searched is described in the following paragraphs and in Attachment
7 "A" (attached hereto and incorporated herein by reference). This affidavit is made in
8 support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A),
9 and 2703(c)(1)(A) to require Google to disclose to the government records and other
10 information in its possession, pertaining to the subscriber or customer associated with
11 the Target Account.

12 2. I am an "investigative or law enforcement officer of the United States"
13 within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of
14 the United States who is empowered by law to conduct investigations of, and to make
15 arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

16 3. I have been employed as a Special Agent of the FBI for approximately five
17 years, which began at the FBI Academy in October 2012. Upon completion of the
18 academy, I was transferred to the Las Vegas Division's white collar crime squad and
19 then the human trafficking squad. Since October 2015, I have been assigned to the Las
20 Vegas Division's violent crime/gang squad. Additionally, I have been a certified member
21 of the FBI's Cellular Analysis Survey Team since August 2015 due to my expertise in
22 the field of historical cell site analysis.

1 4. During my tenure with the FBI, I have conducted surveillance, analyzed
2 telephone records, interviewed witnesses, supervised activities of sources, executed
3 search warrants, executed arrest warrants, and participated in court-authorized
4 interceptions of wire and electronic communications. These investigative activities have
5 been conducted in conjunction with a variety of investigations, to include those involving
6 robbery, drug trafficking, kidnapping, murder, criminal enterprises, and more. In
7 addition to my practical experiences, I received five months of extensive law enforcement
8 training at the FBI Academy.

9 5. The facts in this affidavit are derived from your Affiant's personal
10 observations, his training and experience, and information obtained from other agents,
11 detectives, and witnesses. This affidavit is intended to show merely that there is
12 sufficient probable cause for the requested warrant and does not set forth all of the
13 Affiant's knowledge about this matter.

14 6. Based on your Affiant's training and experience and the facts as set forth
15 in this affidavit, there is probable cause to believe that violations of:

- 16 a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C.A. § 32(a);
17 b. Violence at International Airport - 18 U.S.C. § 37(a)(2); and
18 c. Unlawful Interstate Transport/Delivery of Firearms by Non Federal
19 Firearms Licensee - 18 U.S.C. §§ 922(a)(3) and (5);

20 (hereafter, "Subject Offenses") have been committed by STEPHEN PADDOCK and
21 others yet unknown. There is also probable cause to search the information described in
22 Attachment "A" for evidence of these crimes and information which might reveal the
23
24

1 identities of others involved in these crimes, as described in Attachment "B" (attached
2 hereto and incorporated herein by reference).

3 **PROBABLE CAUSE**

4 7. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music
5 festival, was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At
6 approximately 10:08 p.m., the Las Vegas Metropolitan Police Department (LVMPD)
7 received calls reporting shots had been fired at the concert and multiple victims were
8 struck. LVMPD determined the shots were coming from Rooms 134 and 135 on the 32nd
9 floor of the Mandalay Bay Resort and Casino, located due west of the festival grounds at
10 3950 South Las Vegas Boulevard, Las Vegas, Nevada. These rooms are an elevated
11 position which overlooks the concert venue. Witness statements and video
12 footage captured during the attack indicates that the weapons being used were firing in
13 a fully-automatic fashion.

14 8. LVMPD officers ultimately made entry into the room and located an
15 individual later identified as Stephen Paddock. Paddock was deceased from an apparent
16 self-inflicted gunshot wound.

17 9. Paddock's Nevada driver's license was located in the Mandalay Bay hotel
18 room with Paddock, and both hotel rooms were registered in his name. A player's club
19 card in name of Marilou Danley was located in Paddock's room, and the card returned
20 to the address located on Babbling Brook Street in Mesquite, Nevada. FBI Agents
21 located Danley, who was traveling outside the United States at the time of the
22 shooting. It was ultimately determined that Danley resided with Paddock at the
23 Babbling Brook address.

1 10. On October 2, 2017, search warrants were executed on Paddock's Mandalay
2 Bay hotel rooms, Paddock's vehicle at Mandalay Bay, and two Nevada residences owed
3 by Paddock: 1372 Babbling Brook Court in Mesquite, and 1735 Del Webb Parkway in
4 Reno, Nevada. Officers and Agents found over 20 firearms, hundreds of rounds of
5 ammunition, and hundreds of spent shell casings in the Mandalay Bay hotel rooms, in
6 close proximity to Paddock's body. Over a thousand rounds of rifle ammunition and 100
7 pounds of explosive material was found in Paddock's vehicle. Additional explosive
8 material, approximately 18 firearms, and over 1,000 rounds of ammunition was located
9 at the Mesquite residence. A large quantity of ammunition and multiple firearms were
10 recovered from the Reno residence.

11 11. As of this date, 58 people have been identified to have been killed in
12 Paddock's attack and another 557 were reportedly injured. Additionally, investigators
13 discovered that STEPHEN PADDOCK also utilized a firearm to shoot large fuel tanks
14 on Las Vegas McCarran International Airport property. Multiple bullet holes were found
15 on the tank, which investigators believe was an attempt by STEPHEN PADDOCK to
16 cause the tanks to explode.

17 12. During the execution of the search warrant at the Mandalay Bay hotel room
18 where the attack occurred, three cellular phones were seized. All of the phones are
19 believed to have belonged to STEPHEN PADDOCK. Two of those phones were unlocked
20 and able to be forensically examined. Neither phone contained significant information
21 that allowed investigators to determine the full scope of STEPHEN PADDOCK's
22 planning and preparation for the attack. The other phone, however, a ZTE Model
23 Z837VL bearing IMEI 990006880858377, was locked and investigators do not believe it
24

1 can be forensically examined. Investigators believe the only way to gain access to the
2 content of the locked ZTE phone will be through the authorization to demand
3 information associated with the Target Account from Google, the company which owns
4 the operating system software installed on the phone.

5 13. Your Affiant knows through training and experience that criminals
6 typically make effort to secure and keep hidden information that may incriminate
7 themselves or others. Due to the fact that two of the cellular phones were unlocked and
8 the cellular phone associated with the Target Account was locked, your Affiant believes
9 if there were any information related to a potential conspiracy it would be found within
10 the Target Account.

11 14. Your Affiant believes the requested search warrant will yield significant
12 information from Google such as STEPHEN PADDOCK's contact list, email message
13 content, IP address usage, photographs, third-party applications, and more, which may
14 constitute evidence of his planning of the attack and potentially identify other
15 participants in the attack. Ultimately, your Affiant strongly believes the requested
16 information will lead investigators to determine the full scope of STEPHEN PADDOCK's
17 plan.

18 RELEVANT TECHNICAL TERMS

19 15. The following non-exhaustive list of definitions applies to this Affidavit and
20 the Attachments to this Affidavit:

21 a. The "Internet" is a worldwide network of computer systems operated
22 by governmental entities, corporations, and universities. In order to access the Internet,
23 an individual computer user must subscribe to an access provider, which operates a host
24

1 computer system with direct access to the Internet. The World Wide Web is a
2 functionality of the Internet which allows users of the Internet to share information.

3 b. "Internet Service Providers" are companies that provide access to the
4 Internet. ISPs can also provide other services for their customers including website
5 hosting, email service, remote storage, and co-location of computers and other
6 communications equipment. ISPs offer different ways to access the Internet including
7 telephone-based (dial-up), broadband-based access via a digital subscriber line (DSL) or
8 cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge
9 a fee based upon the type of connection and volume of data (bandwidth). Many ISPs
10 assign each subscriber an account name, such as a user name, an email address, and an
11 email mailbox, and the subscriber typically creates a password for his/her account.

12 c. "ISP Records" are records maintained by ISPs pertaining to their
13 subscribers (regardless of whether those subscribers are individuals or entities). These
14 records may include account application information, subscriber and billing information,
15 account access information (often in the form of log files), emails, information concerning
16 content uploaded and/or stored on the ISP's servers, and other information, which may
17 be stored both in computer data format and in written or printed record format. ISPs
18 reserve and/or maintain computer disk storage space on their computer system for their
19 subscribers' use. This service by ISPs allows for both temporary and long-term storage
20 of electronic communications and many other types of electronic data and files.

21 d. "Online service providers" (also referred to here as "service
22 providers") are companies that provide online services such as email, chat or instant
23 messaging, word processing applications, spreadsheet applications, presentation
24

1 applications similar to PowerPoint, online calendar, photo storage and remote storage
2 services. Sometimes they also can provide web hosting, remote storage, and co-location
3 of computers and other communications equipment. Typically, each service provider
4 assigns each subscriber an account name, such as a user name or screen name and the
5 subscriber typically creates a password for his/her account.

6 e. "Computer," as used herein, is defined as "an electronic, magnetic,
7 optical, electrochemical, or other high speed data processing device performing logical or
8 storage functions, and includes any data storage facility or communications facility
9 directly related to or operating in conjunction with such device."

10 f. A "server" is a centralized computer that provides services for other
11 computers connected to it via a network. The other computers attached to a server are
12 sometimes called "clients." For example, in a large company, it is common for individual
13 employees to have client computers at their desktops. When the employees access their
14 email, or access files stored on the network itself, those files are pulled electronically
15 from the server, where they are stored, and are sent to the client's computer via the
16 network. Notably, servers can be physically stored in any location: it is not uncommon
17 for a network's server to be located hundreds (and even thousands) of miles away from
18 the client computers.

19 g. "Internet Protocol address," or "IP address," refers to a unique
20 number used by a computer to access the Internet. IP addresses can be dynamic,
21 meaning that the Internet Service Provider (ISP) assigns a different unique number to
22 a computer every time it accesses the Internet. IP addresses might also be static, that
23
24

1 is, an ISP assigns a user's computer a particular IP address which is used each time the
2 computer accesses the Internet.

3 h. The term "domain" refers to a word used as a name for computers,
4 networks, services, etc. A domain name typically represents a website, a server computer
5 that hosts that website, or even some computer (or other digital device) connected to the
6 internet. Essentially, when a website (or a server computer that hosts that website) is
7 connected to the internet, it is assigned an IP address. Because IP addresses are difficult
8 for people to remember, domain names are instead used because they are easier to
9 remember than IP addresses. Domain names are formed by the rules and procedures of
10 the Domain Name System (DNS). A common top level domain under these rules is ".com"
11 for commercial organizations, ".gov" for the United States government, and ".org" for
12 organizations. For example, www.usdoj.gov is the domain name that identifies a server
13 used by the U.S. Department of Justice, and which uses IP address of 149.101.46.71.

14 i. "Web hosting services" maintain server computers connected to the
15 Internet. Their customers use those computers to operate websites on the Internet.
16 Customers of web hosting companies place files, software code, databases, and other data
17 on servers. To do this, customers typically connect from their own computers to the
18 server computers across the Internet.

19 j. The term "WhoIs" lookup refers to a search of a publicly available
20 online database that lists information provided when a domain is registered or when an
21 IP address is assigned.

22 k. The terms "communications," "records," "documents," "programs," or
23 "materials" include all information recorded in any form, visual or aural, and by any
24

means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, pictures or videos), or electrical, electronic or magnetic form, as well as digital data files. These terms also include any applications (i.e. software programs). These terms expressly include, among other things, emails, instant messages, chat logs, correspondence attached as to emails (or drafts), calendar entries, buddy lists.

1. "Chat" is usually a real time electronic communication between two or more individuals. Unlike email, which is frequently sent, then read and responded to minutes, hours, or even days later, chats frequently involve an immediate conversation between individuals, similar to a face-to-face conversation. Nearly all chat programs are capable of saving the chat transcript, to enable users to preserve a record of the conversation. By default, some chat programs have this capability enabled, while others do not. Many popular web-based email providers, like Google and Google, provide chat functionality as part of the online services they provide to account holders.

m. "Apps or Applications" are third-party programs that may be installed through the Android operating system, which is owned by Google, for use on a cellular device.

FACTS ABOUT GOOGLE

16. In my training, my experience and this investigation, I have learned that Google owns and operates Android OS, which is an operating system found on many cellular devices to include the device associated with the Target Account. Through this operating system, users can install applications with a variety of functionalities, such as

1 various social media websites, mapping software, banking portals, etc. Records of the
2 applications installed on a specific device are maintained by Google.

3 17. In my training and experience, evidence of which applications were utilized
4 by a specific device can be useful in identifying additional communication facilities,
5 content of communications, financial account information, information related to whom
6 the user associates with, and more. Oftentimes, an individual utilizing a Google account
7 has the option to store certain information located on the device to a cloud, which Google
8 also retains. All of this information can help investigators locate evidence of various
9 criminal activity associated with the user.

10 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

11 18. Your Affiant anticipates executing this warrant under the Electronic
12 Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and
13 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies
14 of the records and other information (including the content of communications)
15 particularly described in Section I of Attachment "B." Upon receipt of the information
16 described in Section I of Attachment "B," government-authorized persons will review
17 that information to locate the items described in Section II of Attachment "B."

18 **CONCLUSION**


19 19. Based on the forgoing, I request that the Court issue the proposed search
20 warrant. This Court has jurisdiction to issue the requested warrant because it is "a court
21 of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A)
22 & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has
23 jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to
24

1 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the
2 service or execution of this warrant.

3 **REQUEST FOR SEALING**

4 20. I further request that the Court order that all papers in support of this
5 application, including the affidavit and search warrant, be sealed until further order of
6 the Court. These documents discuss an ongoing criminal investigation that is neither
7 public nor known to all of the targets of the investigation. Accordingly, there is good
8 cause to seal these documents because their premature disclosure may seriously
9 jeopardize that investigation.

10
11 Respectfully Submitted,

12 
13 _____
14 Ryan S. Burke, Special Agent
Federal Bureau of Investigation

15
16 SWORN TO AND SUBSCRIBED
before me this 16th day of October 2017.

17
18 
19 _____
20 UNITED STATES MAGISTRATE JUDGE
21
22
23
24

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from account inception to present:

- a. The contents of all messages and emails associated with the account, including copies of messages and emails sent to and from the account, draft messages/emails, the source and destination addresses associated with each message/email, the date and time at which each message/email was sent, and the size and length of each message/email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
- d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
- e. All data and contents related to the following Google Services associated with the Target Account: Android; Gmail; Google Calendar; Google Docs; Google Drive; Google Talk; Multilogin; Web History; YouTube; and all other applications.
- f. All information and content associated with any third-party application associated with the Target Account and the dates when the applications were installed;

- 1 g. Based on an analysis of cookies assigned to computers and devices that
2 accessed the Target Account, identify all other Google accounts that have
3 been accessed from any computers and devices that have logged into the
4 Target Account.

5 **II. Information to be seized by the United States**

6 After reviewing all information described in Section I, the United States will seize
7 evidence of violations of Title 18, United States Code Sections 32(a)
8 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
9 International Airport); and 922(a)(3); 5 (Unlawful Interstate Transport/Delivery of
Firearms by Non Federal Firearms Licensee) (the "Subject Offenses") that occur in the
form of the following, from account inception to present:

- 10 a. Communications, transactions and records that may establish ownership
11 and control (or the degree thereof) of the Target Account, including address
12 books, contact or buddy lists, bills, invoices, receipts, registration records,
13 bills, correspondence, notes, records, memoranda, telephone/address books,
14 photographs, video recordings, audio recordings, lists of names, records of
15 payment for access to newsgroups or other online subscription services, and
16 attachments to said communications, transactions and records.
- 17 b. Communications, transactions and records to/from persons who may be co-
18 conspirators of the Subject Offenses, or which may identify co-conspirators.
- 19 c. Communications, transactions and records which may show motivation to
20 commit the Subject Offenses.
- 21 d. Communications, transactions and records that relate to the Subject
22 Offenses.
- 23 e. The terms "communications," "transactions," "records," "documents,"
24 "programs," or "materials" include all information recorded in any form,
visual or aural, and by any means, whether in handmade form (including,
but not limited to, writings, drawings, paintings), photographic form
(including, but not limited to, pictures or videos), or electrical, electronic or
magnetic form, as well as digital data files. These terms also include any
applications (i.e. software programs). These terms expressly include, among
other things, Emails, instant messages, chat logs, correspondence attached
as to Emails (or drafts), calendar entries, buddy lists.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "C"

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

1 5. The search procedures utilized for this review are at the sole discretion of
2 the investigating and prosecuting authorities, and may include the following techniques
(the following is a non-exclusive list, as other search procedures may be used):

3 a. examination of all of the data contained in the Search Warrant Data to view
4 the data and determine whether that data falls within the items to be seized as set forth
herein;

5 b. searching for and attempting to recover from the Search Warrant Data any
6 deleted, hidden, or encrypted data to determine whether that data falls within the list
7 of items to be seized as set forth herein (any data that is encrypted and unreadable will
8 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

9 c. surveying various file directories and the individual files they contain;

10 d. opening files in order to determine their contents;

11 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

12 f. scanning storage areas;

13 g. performing keyword searches through all electronic storage areas to
14 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A; and/or

15 h. performing any other data analysis technique that may be necessary to
16 locate and retrieve the evidence described in Attachment B, Section II.

17 **Return and Review Procedures**

18 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

19 (e) Issuing the Warrant.

20 (2) Contents of the Warrant.

21 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
22 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
23 be returned. The warrant must command the officer to:

1 (i) execute the warrant within a specified time no longer than 14 days;

2 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
3 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
4 copying of electronically stored information. Unless otherwise specified, the warrant
5 authorizes a later review of the media or information consistent with the warrant. The
6 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
7 on-site copying of the media or information, and not to any later off-site copying or
8 review.

6 (f) Executing and Returning the Warrant.

7 (1) Warrant to Search for and Seize a Person or Property.

8 (B) Inventory. An officer present during the execution of the warrant must prepare
9 and verify an inventory of any property seized. . . . In a case involving the seizure of
10 electronic storage media or the seizure or copying of electronically stored information,
11 the inventory may be limited to describing the physical storage media that were seized
12 or copied. The officer may retain a copy of the electronically stored information that was
13 seized or copied.

12 7. Pursuant to this Rule, the government understands and will act in
13 accordance with the following:

14 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
15 of the warrant, an agent is required to file an inventory return with the Court, that is,
16 to file an itemized list of the property seized. Execution of the warrant begins when
17 the United States serves the warrant on the named custodian; execution is complete
18 when the custodian provides all Search Warrant Data to the United States. Within
19 fourteen (14) days of completion of the execution of the warrant, the inventory will be
20 filed.

18 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
19 which the electronically stored information must be seized after the issuance of the
20 warrant and copied after the execution of the warrant, not the "later review of the media
21 or information" seized, or the later off-site digital copying of that media.

21 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
22 may be limited to a description of the "physical storage media" into which the Search
23 Warrant Data that was seized was placed, not an itemization of the information or data
24 stored on the "physical storage media" into which the Search Warrant Data was placed;

1 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
2 purposes of the investigation. The government proposes that the original storage media
3 on which the Search Warrant Data was placed plus a full image copy of the seized Search
Warrant Data be retained by the government.

4 e. If the person from whom any Search Warrant Data was seized requests the return
5 of any information in the Search Warrant Data that is not set forth in Attachment B,
6 Section II, that information will be copied onto appropriate media and returned to the
7 person from whom the information was seized.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

UNITED STATES DISTRICT COURT

for the
District of Nevada

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

MARILOUROSES@LIVE.COM A2

Case No. 2:17-mj- 967-NJK

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENTS B and C

YOU ARE COMMANDED to execute this warrant on or before October 20, 2017 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Nancy J. Koppe
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 10/6/2017 7:50pm

City and state: Las Vegas, Nevada

Judge's signature

Printed name and title

Nancy J. Koppe US Magistrate Judge

1 ATTACHMENT "A2"

2 ONLINE ACCOUNT TO BE SEARCHED

3 1. This warrant applies to information associated with the Microsoft email
4 account marilouroses@live.com (the "Target Accounts") from their inception to present,
5 which is stored at premises owned, maintained, controlled, or operated by Microsoft
6 Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

23 ATTACHMENT "B"

24 Particular Things to be Seized

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachment A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A1 and A2 from account inception to present:

- a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
- d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
- e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Microsoft-related facility.

II. Information to be seized by the United States

1
2 After reviewing all information described in Section I, the United States will seize
3 evidence of violations of Title 18, United States Code Sections 32(a)
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
5 International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of
6 Firearms by Non Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject
7 Offenses") that occur in the form of the following, from account inception to present:
8

- 9
- 10 a. Communications, transactions and records that may establish ownership
11 and control (or the degree thereof) of the Target Account, including address
12 books, contact or buddy lists, bills, invoices, receipts, registration records,
13 bills, correspondence, notes, records, memoranda, telephone/address books,
14 photographs, video recordings, audio recordings, lists of names, records of
15 payment for access to newsgroups or other online subscription services, and
16 attachments to said communications, transactions and records.
 - 17 b. Communications, transactions and records to/from persons who may be co-
18 conspirators of the Subject Offenses, or which may identify co-conspirators.
 - 19 c. Communications, transactions and records which may show motivation to
20 commit the Subject Offenses.
 - 21 d. Communications, transactions and records that relate to the Subject
22 Offenses.
 - 23 e. The terms "communications," "transactions," "records," "documents,"
24 "programs," or "materials" include all information recorded in any form,
visual or aural, and by any means, whether in handmade form (including,
but not limited to, writings, drawings, paintings), photographic form
(including, but not limited to, pictures or videos), or electrical, electronic or
magnetic form, as well as digital data files. These terms also include any
applications (i.e. software programs). These terms expressly include, among
other things, Emails, instant messages, chat logs, correspondence attached
as to Emails (or drafts), calendar entries, buddy lists.

ATTACHMENT "C"

1 **PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED**
2 **PURSUANT TO THIS SEARCH WARRANT**

3 1. In executing this warrant, the government must make reasonable efforts to
4 use methods and procedures that will locate and expose in the electronic data produced
5 in response to this search warrant ("the Search Warrant Data") those categories of data,
6 files, documents, or other electronically stored information that are identified with
7 particularity in the warrant, while minimizing exposure or examination of irrelevant,
8 privileged, or confidential files to the extent reasonably practicable.

9 2. When the Search Warrant Data is received, the government will make a
10 duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The
11 original version of the Search Warrant Data will be sealed and preserved for purposes
12 of: later judicial review or order to return or dispose of the Search Warrant Data;
13 production to the defense in any criminal case if authorized by statute, rule, or the
14 Constitution; for purposes of showing the chain of custody of the Search Warrant Data
15 and the Search Warrant Data Copy; or for any other lawful purpose. The original of the
16 Search Warrant Data will not be searched or examined except to ensure that it has been
17 fully and completely replicated in the Search Warrant Data Copy.

18 3. The investigating agents will then search the entirety of the Search
19 Warrant Data Copy using any and all methods and procedures deemed appropriate by
20 the United States designed to identify the information listed as Information to be Seized
21 in Attachment B, Section II. The United States may copy, extract or otherwise segregate
22 information or data listed as Information to be Seized in Attachment B, Section II.
23 Information or data so copied, extracted or otherwise segregated will no longer be subject
24 to any handling restrictions that might be set out in this protocol beyond those required
25 by binding law. To the extent evidence of crimes not within the scope of this warrant
26 appear in plain view during this review, a supplemental or "piggyback" warrant will be
27 applied for in order to further search that document, data, or other item.

28 4. Once the Search Warrant Data Copy has been thoroughly and completely
29 examined for any document, data, or other items identified in Attachment B, Section II
30 as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject
31 to any further search or examination unless authorized by another search warrant or
32 other appropriate court order. The Search Warrant Data Copy will be held and preserved
33 for the same purposes identified above in Paragraph 2.

34 5. The search procedures utilized for this review are at the sole discretion of
35 the investigating and prosecuting authorities, and may include the following techniques
36 (the following is a non-exclusive list, as other search procedures may be used):

1 a. examination of all of the data contained in the Search Warrant Data to view
2 the data and determine whether that data falls within the items to be seized as set forth
herein;

3 b. searching for and attempting to recover from the Search Warrant Data any
4 deleted, hidden, or encrypted data to determine whether that data falls within the list
5 of items to be seized as set forth herein (any data that is encrypted and unreadable will
6 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

7 c. surveying various file directories and the individual files they contain;

8 d. opening files in order to determine their contents;

9 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

10 f. scanning storage areas;

11 g. performing keyword searches through all electronic storage areas to
12 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A1 and A2; and/or

13 h. performing any other data analysis technique that may be necessary to
14 locate and retrieve the evidence described in Attachment B, Section II.

15 Return and Review Procedures

16 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

17 (e) Issuing the Warrant.

18 (2) Contents of the Warrant.

19 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
20 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
21 be returned. The warrant must command the officer to:

22 (i) execute the warrant within a specified time no longer than 14 days;

23 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
24

1 copying of electronically stored information. Unless otherwise specified, the warrant
2 authorizes a later review of the media or information consistent with the warrant. The
3 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
on-site copying of the media or information, and not to any later off-site copying or
review.

4 (f) Executing and Returning the Warrant.

5 (1) Warrant to Search for and Seize a Person or Property.

6 (B) Inventory. An officer present during the execution of the warrant must prepare
7 and verify an inventory of any property seized. . . . In a case involving the seizure of
8 electronic storage media or the seizure or copying of electronically stored information,
the inventory may be limited to describing the physical storage media that were seized
9 or copied. The officer may retain a copy of the electronically stored information that was
seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in
accordance with the following:

11 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
12 of the warrant, an agent is required to file an inventory return with the Court, that is,
to file an itemized list of the property seized. Execution of the warrant begins when
13 the United States serves the warrant on the named custodian; execution is complete
when the custodian provides all Search Warrant Data to the United States. Within
14 fourteen (14) days of completion of the execution of the warrant, the inventory will be
15 filed.

16 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
which the electronically stored information must be seized after the issuance of the
17 warrant and copied after the execution of the warrant, not the "later review of the media
or information" seized, or the later off-site digital copying of that media.

18 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
19 may be limited to a description of the "physical storage media" into which the Search
Warrant Data that was seized was placed, not an itemization of the information or data
20 stored on the "physical storage media" into which the Search Warrant Data was placed;

21 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
22 purposes of the investigation. The government proposes that the original storage media
on which the Search Warrant Data was placed plus a full image copy of the seized Search
23 Warrant Data be retained by the government.

1 e. If the person from whom any Search Warrant Data was seized requests the return
2 of any information in the Search Warrant Data that is not set forth in Attachment B,
3 Section II, that information will be copied onto appropriate media and returned to the
4 person from whom the information was seized.
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24



SEALED

Office of the United States Attorney
District of Nevada
501 Las Vegas Boulevard, Suite 1100
Las Vegas, Nevada 89101
(702) 388-6336

STEVEN W. MYHRE
Acting United States Attorney
District of Nevada
CRISTINA D. SILVA
PATRICK BURNS
Assistant United States Attorneys
501 Las Vegas Blvd. South, Ste. 1100
Las Vegas, Nevada 89101
Telephone: (702) 388-6336
Fax (702) 388-6698
john.p.burns@usdoj.gov

Attorney for the United States of America

**UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA**

-oOo-

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
EMAIL ACCOUNTS
CENTRALPARK1@LIVE.COM THAT IS
STORED AT A PREMISES
CONTROLLED BY MICROSOFT. A1

Magistrate No.

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH
WARRANTS**

(Under Seal)

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
EMAIL ACCOUNTS
MARILOUROSES@LIVE.COM THAT IS
STORED AT A PREMISES
CONTROLLED BY MICROSOFT. A2

Magistrate No. 17-mj-967-NJK

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH
WARRANTS**

(Under Seal)

STATE OF NEVADA)
) ss:
COUNTY OF CLARK)

1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8
9
0
1
2
3
4

2
3
4

5

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

22
23
24

1 the United States who is empowered by law to conduct investigations of, and to make
2 arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

3 3. I have been employed as a Special Agent of the FBI for approximately five
4 years, which began at the FBI Academy in October 2012. Upon completion of the
5 academy, I was transferred to the Las Vegas Division's white collar crime squad and
6 then the human trafficking squad. Since October 2015, I have been assigned to the Las
7 Vegas Division's violent crime/gang squad. Additionally, I have been a certified member
8 of the FBI's Cellular Analysis Survey Team since August 2015 due to my expertise in
9 the field of historical cell site analysis.

10 4. During my tenure with the FBI, I have conducted surveillance, analyzed
11 telephone records, interviewed witnesses, supervised activities of sources, executed
12 search warrants, executed arrest warrants, and participated in court-authorized
13 interceptions of wire and electronic communications. These investigative activities have
14 been conducted in conjunction with a variety of investigations, to include those involving
15 robbery, drug trafficking, kidnapping, murder, criminal enterprises, and more. In
16 addition to my practical experiences, I received five months of extensive law enforcement
17 training at the FBI Academy.

18 5. The facts in this affidavit are derived from your Affiant's personal
19 observations, his training and experience, and information obtained from other agents,
20 detectives, and witnesses. This affidavit is intended to show merely that there is
21 sufficient probable cause for the requested warrants and does not set forth all of the
22 Affiant's knowledge about this matter.

1 6. Based on your Affiant's training and experience and the facts as set forth
2 in this affidavit, there is probable cause to believe that violations of:

- 3 a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C.A. § 32(a);
4 b. Violence at International Airport - 18 U.S.C. § 37(a)(2); and
5 c. Unlawful Interstate Transport/Delivery of Firearms by Non Federal
6 Firearms Licensee – 18 U.S.C. §§ 922(a)(3) and (5);
7 d. Aiding and Abetting – 18 U.S.C. § 2.

8 (hereafter, "Subject Offenses") have been committed by STEPHEN PADDOCK,
9 MARILOU DANLEY, and others yet unknown. There is also probable cause to search
10 the information described in Attachment "A" for evidence of these crimes and
11 information which might reveal the identities of others involved in these crimes, as
12 described in Attachment "B" (attached hereto and incorporated herein by reference).

13 **PROBABLE CAUSE**

14 7. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music
15 festival, was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At
16 approximately 10:08 p.m., the Las Vegas Metropolitan Police Department (LVMPD)
17 received calls reporting shots had been fired at the concert and multiple victims were
18 struck. LVMPD determined the shots were coming from Rooms 134 and 135 on the 32nd
19 floor of the Mandalay Bay Resort and Casino, located due west of the festival rounds at
20 3950 South Las Vegas Boulevard, Las Vegas, Nevada. These rooms are an elevated
21 position which overlooks the concert venue. Witness statements and video
22 footage captured during the attack indicates that the weapons being used were firing in
23 a fully-automatic fashion.
24

1 8. LVMPD officers ultimately made entry into the room and located an
2 individual later identified as Stephen Paddock. Paddock was deceased from an apparent
3 self-inflicted gunshot wound.

4 9. Paddock's Nevada driver's license was located in the Mandalay Bay hotel
5 room with Paddock, and both hotel rooms were registered in his name. A player's club
6 card in name of Marilou Danley was located in Paddock's room, and the card returned
7 to the address located on Babbling Brook Street in Mesquite, Nevada. FBI Agents
8 located Danley, who was traveling outside the United States at the time of the
9 shooting. It was ultimately determined that Danley resided with Paddock at the
10 Babbling Brook address.

11 10. On October 2, 2017, search warrants were executed on Paddock's Mandalay
12 Bay hotel rooms, Paddock's vehicle at Mandalay Bay, and two Nevada residences owed
13 by Paddock: 1372 Babbling Brook Court in Mesquite, and 1735 Del Webb Parkway in
14 Reno, Nevada. Officers and Agents found over 20 firearms, hundreds of rounds of
15 ammunition, and hundreds of spent shell casings in the Mandalay Bay hotel rooms, in
16 close proximity to Paddock's body. Over a thousand rounds of rifle ammunition and 100
17 pounds of explosive material was found in Paddock's vehicle. Additional explosive
18 material, approximately 18 firearms, and over 1,000 rounds of ammunition was located
19 at the Mesquite residence. A large quantity of ammunition and multiple firearms were
20 recovered from the Reno residence.

21 11. As of this date, 58 people have been identified to have been killed in
22 Paddock's attack and another 557 were reportedly injured. Additionally, investigators
23 discovered that STEPHEN PADDOCK also utilized a firearm to shoot large fuel tanks
24

1 on Las Vegas McCarran International Airport property. Multiple bullet holes were found
2 on the tank, which investigators believe was an attempt by STEPHEN PADDOCK to
3 cause the tanks to explode.

4 12. In an effort to determine whether or not STEPHEN PADDOCK was
5 assisted and/or conspired with unknown individuals, investigators have attempted to
6 identify all of STEPHEN PADDOCK's associated. It was quickly determined that a
7 casino player's card in the name of MARILOU DANLEY was located in the room at the
8 time of the attack. She has been identified thus far as the most likely person who aided
9 or abetted STEPHEN PADDOCK based on her informing law enforcement that her
10 fingerprints would likely be found on the ammunition used during the attack.
11 Subsequently, investigators worked to identify the communication facilities utilized by
12 STEPHEN PADDOCK and MARILOU DANLEY.

13 13. Based on a review of STEPHEN PADDOCK's financial accounts, Target
14 Account 1 was determined to belong to STEPHEN PADDOCK. On October 3, 2017,
15 investigators requested an emergency disclosure of records from Microsoft related to
16 Target Account 1 so it could be immediately searched for any evidence of additional co-
17 conspirators. Unfortunately, the information was only requested for a six month
18 timeframe. Within the account, investigators identified Target Account 2 as one that
19 belonged to MARILOU DANLEY, which was clear based on the communications
20 between the two email accounts.

21 14. On September 25, 2017, an email was exchanged between the Target
22 Accounts which discussed a wire transfer of funds which was to be sent by STEPHEN
23
24

1 PADDOCK to MARILOU DANLEY. It is unclear what the purpose of the wire transfer
2 was, but MARILOU DANLEY is known to have been in the Philippines at the time.

3 15. Additionally, on July 6, 2017, Target Account 1 sent an email to
4 centralpark4804@gmail.com which read, "try an ar before u buy. we have huge selection.
5 located in the las vegas area." Later that day, an email was received back from
6 centralpark4804@gmail.com to Target Account 1 that read, "we have a wide variety of
7 optics and ammunition to try." And lastly, Target Account 1 later sent an email to
8 centralpark4804@gmail.com that read, "for a thrill try out bumpfire ar's with a 100
9 round magazine." Investigators believe these communications may have been related to
10 the eventual attack that occurred at the Mandalay Bay in Las Vegas.

11 16. Your Affiant believes the requested search warrants will yield significant
12 information from Microsoft such as STEPHEN PADDOCK's and MARILOU DANLEY's
13 contact lists, email messages content, IP address usage, photographs, third-party
14 applications associated with the account, and more, which may constitute evidence of
15 the planning of the attack and potentially identify other participants in the attack.
16 Ultimately, your Affiant strongly believes the requested information will lead
17 investigators to determine the full scope of STEPHEN PADDOCK's plan and MARILOU
18 DANLEY's possible involvement.

19 RELEVANT TECHNICAL TERMS

20 17. The following non-exhaustive list of definitions applies to this Affidavit and
21 the Attachments to this Affidavit:

22 a. The "Internet" is a worldwide network of computer systems operated
23 by governmental entities, corporations, and universities. In order to access the Internet,
24

1 an individual computer user must subscribe to an access provider, which operates a host
2 computer system with direct access to the Internet. The World Wide Web is a
3 functionality of the Internet which allows users of the Internet to share information.

4 b. "Internet Service Providers" are companies that provide access to the
5 Internet. ISPs can also provide other services for their customers including website
6 hosting, email service, remote storage, and co-location of computers and other
7 communications equipment. ISPs offer different ways to access the Internet including
8 telephone-based (dial-up), broadband-based access via a digital subscriber line (DSL) or
9 cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge
10 a fee based upon the type of connection and volume of data (bandwidth). Many ISPs
11 assign each subscriber an account name, such as a user name, an email address, and an
12 email mailbox, and the subscriber typically creates a password for his/her account.

13 c. "ISP Records" are records maintained by ISPs pertaining to their
14 subscribers (regardless of whether those subscribers are individuals or entities). These
15 records may include account application information, subscriber and billing information,
16 account access information (often in the form of log files), emails, information concerning
17 content uploaded and/or stored on the ISP's servers, and other information, which may
18 be stored both in computer data format and in written or printed record format. ISPs
19 reserve and/or maintain computer disk storage space on their computer system for their
20 subscribers' use. This service by ISPs allows for both temporary and long-term storage
21 of electronic communications and many other types of electronic data and files.

22 d. "Online service providers" (also referred to here as "service
23 providers") are companies that provide online services such as email, chat or instant
24

1 messaging, word processing applications, spreadsheet applications, presentation
2 applications similar to PowerPoint, online calendar, photo storage and remote storage
3 services. Sometimes they also can provide web hosting, remote storage, and co-location
4 of computers and other communications equipment. Typically, each service provider
5 assigns each subscriber an account name, such as a user name or screen name and the
6 subscriber typically creates a password for his/her account.

7 e. "Computer," as used herein, is defined as "an electronic, magnetic,
8 optical, electrochemical, or other high speed data processing device performing logical or
9 storage functions, and includes any data storage facility or communications facility
10 directly related to or operating in conjunction with such device."

11 f. A "server" is a centralized computer that provides services for other
12 computers connected to it via a network. The other computers attached to a server are
13 sometimes called "clients." For example, in a large company, it is common for individual
14 employees to have client computers at their desktops. When the employees access their
15 email, or access files stored on the network itself, those files are pulled electronically
16 from the server, where they are stored, and are sent to the client's computer via the
17 network. Notably, servers can be physically stored in any location: it is not uncommon
18 for a network's server to be located hundreds (and even thousands) of miles away from
19 the client computers.

20 g. "Internet Protocol address," or "IP address," refers to a unique
21 number used by a computer to access the Internet. IP addresses can be dynamic,
22 meaning that the Internet Service Provider (ISP) assigns a different unique number to
23 a computer every time it accesses the Internet. IP addresses might also be static, that
24

1 is, an ISP assigns a user's computer a particular IP address which is used each time the
2 computer accesses the Internet.

3 h. The term "domain" refers to a word used as a name for computers,
4 networks, services, etc. A domain name typically represents a website, a server computer
5 that hosts that website, or even some computer (or other digital device) connected to the
6 internet. Essentially, when a website (or a server computer that hosts that website) is
7 connected to the internet, it is assigned an IP address. Because IP addresses are difficult
8 for people to remember, domain names are instead used because they are easier to
9 remember than IP addresses. Domain names are formed by the rules and procedures of
10 the Domain Name System (DNS). A common top level domain under these rules is ".com"
11 for commercial organizations, ".gov" for the United States government, and ".org" for
12 organizations. For example, www.usdoj.gov is the domain name that identifies a server
13 used by the U.S. Department of Justice, and which uses IP address of 149.101.46.71.

14 i. "Web hosting services" maintain server computers connected to the
15 Internet. Their customers use those computers to operate websites on the Internet.
16 Customers of web hosting companies place files, software code, databases, and other data
17 on servers. To do this, customers typically connect from their own computers to the
18 server computers across the Internet.

19 j. The term "WhoIs" lookup refers to a search of a publicly available
20 online database that lists information provided when a domain is registered or when an
21 IP address is assigned.

22 k. The terms "communications," "records," "documents," "programs," or
23 "materials" include all information recorded in any form, visual or aural, and by any
24

1 means, whether in handmade form (including, but not limited to, writings, drawings,
2 paintings), photographic form (including, but not limited to, pictures or videos), or
3 electrical, electronic or magnetic form, as well as digital data files. These terms also
4 include any applications (i.e. software programs). These terms expressly include, among
5 other things, emails, instant messages, chat logs, correspondence attached as to emails
6 (or drafts), calendar entries, buddy lists.

7 1. "Chat" is usually a real time electronic communication between two
8 or more individuals. Unlike email, which is frequently sent, then read and responded to
9 minutes, hours, or even days later, chats frequently involve an immediate conversation
10 between individuals, similar to a face-to-face conversation. Nearly all chat programs are
11 capable of saving the chat transcript, to enable users to preserve a record of the
12 conversation. By default, some chat programs have this capability enabled, while others
13 do not. Many popular web-based email providers, like Microsoft and Microsoft, provide
14 chat functionality as part of the online services they provide to account holders.

15 **FACTS ABOUT EMAIL PROVIDERS**

16 18. In my training, my experience and this investigation, I have learned that
17 Microsoft (the Service Provider) is a company that provides free web-based Internet
18 email access to the general public, and that stored electronic communications, including
19 opened and unopened email for Microsoft subscribers may be located on the computers
20 of Microsoft. I have also learned that Microsoft Inc. provides various on-line service
21 messaging services to the general public. Instant Messaging ("IM") is a form of real-time
22 direct text-based communication between two or more people using shared clients. The
23 text is conveyed via devices connected over a network such as the Internet. In addition
24

1 to text, Microsoft's software allows users with the most current updated versions to
2 utilize its webcam service. This option enables users from distances all over the world to
3 view others who have installed a webcam on their end. Thus, the Service Provider's
4 servers will contain a wide variety of the subscriber's files, including emails, address
5 books, contact or buddy lists, calendar data, pictures, chat logs, and other files.

6 19. To use these services, subscribers register for online accounts like the
7 Target Accounts. During the registration process, service providers such as the ones here
8 ask subscribers to provide basic personal information. This information can include the
9 subscriber's full name, physical address, telephone numbers and other identifiers,
10 alternative email addresses, and, for paying subscribers, means and source of payment
11 (including any credit card or bank account number). Based on my training and my
12 experience, I know that subscribers may insert false information to conceal their
13 identity; even if this proves to be the case, however, I know that this information often
14 provide clues to their identity, location or illicit activities.

15 20. In general, when a subscriber receives an email, it is typically stored in the
16 subscriber's "mail box" on that service provider's servers until the subscriber deletes the
17 Email. If the subscriber does not delete the message, the message (and any attachments)
18 can remain on that service provider's servers indefinitely.

19 21. Similarly, when the subscriber sends an email, it is initiated at the
20 subscriber's computer, transferred via the Internet to the service provider's servers, and
21 then transmitted to its end destination. That service provider often saves a copy of the
22 email sent. Unless the sender of the email specifically deletes the Email from the
23 provider's server, the email can remain on the system indefinitely.

1 22. A sent or received email typically includes the content of the message,
2 source and destination addresses, the date and time at which the email was sent, and
3 the size and length of the email. If an email user writes a draft message but does not
4 send it, that message may also be saved by that service provider, but may not include all
5 of these categories of data.

6 23. Just as a computer on a desk can be used to store a wide variety of files, so
7 can online accounts, such as the accounts subject to this application. First, subscribers
8 can store many types of files as attachments to emails in online accounts. Second,
9 because service providers provide the services listed above (e.g. word processing,
10 spreadsheets, pictures), subscribers who use these services usually store documents on
11 servers maintained and/or owned by service providers. Thus, these online accounts often
12 contain documents such as pictures, audio or video recordings, logs, spreadsheets,
13 applications and other files.

14 24. Reviewing files stored in online accounts raises many of the same
15 difficulties as with reviewing files stored on a local computer. For example, based on my
16 training, my experience and this investigation, I know that subscribers of these online
17 services can conceal their activities by altering files before they upload them to the online
18 service. Subscribers can change file names to more innocuous sounding names (e.g.
19 renaming "FraudRecords.doc" to "ChristmasList.doc"), they can change file extensions
20 to make one kind of file appear like a different type of file (e.g. changing the spreadsheet
21 "StolenCreditProfiles.xls" to "FamilyPhoto.jpg" to appear to be a picture file, where the
22 file extension ".xls" denotes an Excel spreadsheet file and ".jpg" a JPEG format image
23 file), or they can change the times and dates a file was last accessed or modified by
24

1 changing a computer's system time/date and then uploading that file to the Online
2 Accounts. Thus, to detect any files that the subscriber may have concealed, agents will
3 need to review all of the files in the Target Accounts; they will, however, only seize the
4 items that the Court authorizes to be seized. Similarly, subscribers can conceal their
5 activities by encrypting files. Thus, these files may need to be decrypted to detect
6 whether it constitutes an Item to be Seized.

7 25. I also believe that people engaged in crimes such as the one described
8 herein often use online accounts because they give people engaged in these crimes a way
9 to easily communicate with other co-conspirators. Moreover, online accounts are easily
10 concealed from law enforcement. Unlike physical documents, electronic documents can
11 be stored in a physical place far away, where they are less likely to be discovered.

12 26. Service providers typically retain certain transactional information about
13 the creation and use of each account on their systems. This information can include the
14 date on which the account was created, the length of service, records of log-in (i.e.,
15 session) times and durations, the types of service utilized, the status of the account
16 (including whether the account is inactive or closed), the methods used to connect to the
17 account (such as logging into the account via websites controlled by the Service
18 Provider), and other log files that reflect usage of the account. In addition, service
19 providers often have records of the Internet Protocol address ("IP address") used to
20 register the account and the IP addresses associated with particular logins to the
21 account. Because every device that connects to the Internet must use an IP address, IP
22 address information can help to identify which computers or other devices were used to
23 access the online account.

1 27. In some cases, subscribers will communicate directly with a service
2 provider about issues relating to the account, such as technical problems, billing
3 inquiries, or complaints from or about other users. Service providers typically retain
4 records about such communications, including records of contacts between the user and
5 the provider's support services, as well records of any actions taken by the provider or
6 user as a result of the communications.

7 28. In my training and experience, evidence of who was using an online
8 account may be found in address books, contact or buddy lists, emails in the account,
9 and pictures and files, whether stored as attachments or in the suite of the service
10 provider's online applications. Therefore, the computers of the Service Providers are
11 likely to contain stored electronic communications (including retrieved and un-retrieved
12 email for their subscribers) and information concerning subscribers and their use of the
13 provider's services, such as account access information, email transaction information,
14 documents, pictures, and account application information.

15 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

16 29. Your Affiant anticipates executing these warrants under the Electronic
17 Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and
18 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government
19 copies of the records and other information (including the content of communications)
20 particularly described in Section I of Attachment "B." Upon receipt of the information
21 described in Section I of Attachment "B," government-authorized persons will review
22 that information to locate the items described in Section II of Attachment "B."

23 **CONCLUSION**

30. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

31. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully Submitted,

Ryan S. Burke, Special Agent
Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED
before me this 6th day of October 2017.

UNITED STATES MAGISTRATE JUDGE

1 ATTACHMENT "A1"

2 ONLINE ACCOUNT TO BE SEARCHED

3 1. This warrant applies to information associated with the Microsoft email
4 account centralpark1@live.com (the "Target Accounts") from their inception to present,
5 which is stored at premises owned, maintained, controlled, or operated by Microsoft
6 Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

1 ATTACHMENT "A2"

2 ONLINE ACCOUNT TO BE SEARCHED

3 1. This warrant applies to information associated with the Microsoft email
4 account marilouroses@live.com (the "Target Accounts") from their inception to present,
5 which is stored at premises owned, maintained, controlled, or operated by Microsoft
6 Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

ATTACHMENT "B"
Particular Things to be Seized

I. Information to be disclosed by the Service Provider

To the extent that the information described in Attachment A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A1 and A2 from account inception to present:

- a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
- d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
- e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Microsoft-related facility.

II. Information to be seized by the United States

1
2 After reviewing all information described in Section I, the United States will seize
3 evidence of violations of Title 18, United States Code Sections 32(a)
4 (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at
5 International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of
6 Firearms by Non Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject
7 Offenses") that occur in the form of the following, from account inception to present:

- 8
- 9 a. Communications, transactions and records that may establish ownership
10 and control (or the degree thereof) of the Target Account, including address
11 books, contact or buddy lists, bills, invoices, receipts, registration records,
12 bills, correspondence, notes, records, memoranda, telephone/address books,
13 photographs, video recordings, audio recordings, lists of names, records of
14 payment for access to newsgroups or other online subscription services, and
15 attachments to said communications, transactions and records.
 - 16 b. Communications, transactions and records to/from persons who may be co-
17 conspirators of the Subject Offenses, or which may identify co-conspirators.
 - 18 c. Communications, transactions and records which may show motivation to
19 commit the Subject Offenses.
 - 20 d. Communications, transactions and records that relate to the Subject
21 Offenses.
 - 22 e. The terms "communications," "transactions," "records," "documents,"
23 "programs," or "materials" include all information recorded in any form,
24 visual or aural, and by any means, whether in handmade form (including,
but not limited to, writings, drawings, paintings), photographic form
(including, but not limited to, pictures or videos), or electrical, electronic or
magnetic form, as well as digital data files. These terms also include any
applications (i.e. software programs). These terms expressly include, among
other things, Emails, instant messages, chat logs, correspondence attached
as to Emails (or drafts), calendar entries, buddy lists.

ATTACHMENT "C"

1 **PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED**
2 **PURSUANT TO THIS SEARCH WARRANT**

3 1. In executing this warrant, the government must make reasonable efforts to
4 use methods and procedures that will locate and expose in the electronic data produced
5 in response to this search warrant ("the Search Warrant Data") those categories of data,
6 files, documents, or other electronically stored information that are identified with
7 particularity in the warrant, while minimizing exposure or examination of irrelevant,
8 privileged, or confidential files to the extent reasonably practicable.

9 2. When the Search Warrant Data is received, the government will make a
10 duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The
11 original version of the Search Warrant Data will be sealed and preserved for purposes
12 of: later judicial review or order to return or dispose of the Search Warrant Data;
13 production to the defense in any criminal case if authorized by statute, rule, or the
14 Constitution; for purposes of showing the chain of custody of the Search Warrant Data
15 and the Search Warrant Data Copy; or for any other lawful purpose. The original of the
16 Search Warrant Data will not be searched or examined except to ensure that it has been
17 fully and completely replicated in the Search Warrant Data Copy.

18 3. The investigating agents will then search the entirety of the Search
19 Warrant Data Copy using any and all methods and procedures deemed appropriate by
20 the United States designed to identify the information listed as Information to be Seized
21 in Attachment B, Section II. The United States may copy, extract or otherwise segregate
22 information or data listed as Information to be Seized in Attachment B, Section II.
23 Information or data so copied, extracted or otherwise segregated will no longer be subject
24 to any handling restrictions that might be set out in this protocol beyond those required
 by binding law. To the extent evidence of crimes not within the scope of this warrant
 appear in plain view during this review, a supplemental or "piggyback" warrant will be
 applied for in order to further search that document, data, or other item.

 4. Once the Search Warrant Data Copy has been thoroughly and completely
examined for any document, data, or other items identified in Attachment B, Section II
as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject
to any further search or examination unless authorized by another search warrant or
other appropriate court order. The Search Warrant Data Copy will be held and preserved
for the same purposes identified above in Paragraph 2.

 5. The search procedures utilized for this review are at the sole discretion of
the investigating and prosecuting authorities, and may include the following techniques
(the following is a non-exclusive list, as other search procedures may be used):

1 a. examination of all of the data contained in the Search Warrant Data to view
2 the data and determine whether that data falls within the items to be seized as set forth
herein;

3 b. searching for and attempting to recover from the Search Warrant Data any
4 deleted, hidden, or encrypted data to determine whether that data falls within the list
5 of items to be seized as set forth herein (any data that is encrypted and unreadable will
6 not be returned unless law enforcement personnel have determined that the data is not
(1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband,
(4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

7 c. surveying various file directories and the individual files they contain;

8 d. opening files in order to determine their contents;

9 e. using hash values to narrow the scope of what may be found. Hash values
are under- inclusive, but are still a helpful tool;

10 f. scanning storage areas;

11 g. performing keyword searches through all electronic storage areas to
12 determine whether occurrences of language contained in such storage areas exist that
are likely to appear in the evidence described in Attachment A1 and A2; and/or

13 h. performing any other data analysis technique that may be necessary to
14 locate and retrieve the evidence described in Attachment B, Section II.

15 **Return and Review Procedures**

16 6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant
part:

17 (e) Issuing the Warrant.

18 (2) Contents of the Warrant.

19 (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-
20 device warrant, the warrant must identify the person or property to be searched, identify
any person or property to be seized, and designate the magistrate judge to whom it must
21 be returned. The warrant must command the officer to:

22 (i) execute the warrant within a specified time no longer than 14 days;

23 (B) Warrant Seeking Electronically Stored Information. A warrant under Rule
41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or
24

1 copying of electronically stored information. Unless otherwise specified, the warrant
2 authorizes a later review of the media or information consistent with the warrant. The
3 time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or
on-site copying of the media or information, and not to any later off-site copying or
review.

4 (f) Executing and Returning the Warrant.

5 (1) Warrant to Search for and Seize a Person or Property.

6 (B) Inventory. An officer present during the execution of the warrant must prepare
7 and verify an inventory of any property seized. . . . In a case involving the seizure of
8 electronic storage media or the seizure or copying of electronically stored information,
the inventory may be limited to describing the physical storage media that were seized
9 or copied. The officer may retain a copy of the electronically stored information that was
seized or copied.

10 7. Pursuant to this Rule, the government understands and will act in
accordance with the following:

11 a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution
12 of the warrant, an agent is required to file an inventory return with the Court, that is,
to file an itemized list of the property seized. Execution of the warrant begins when
13 the United States serves the warrant on the named custodian; execution is complete
when the custodian provides all Search Warrant Data to the United States. Within
14 fourteen (14) days of completion of the execution of the warrant, the inventory will be
15 filed.

16 b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within
which the electronically stored information must be seized after the issuance of the
17 warrant and copied after the execution of the warrant, not the "later review of the media
or information" seized, or the later off-site digital copying of that media.

18 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court
19 may be limited to a description of the "physical storage media" into which the Search
Warrant Data that was seized was placed, not an itemization of the information or data
20 stored on the "physical storage media" into which the Search Warrant Data was placed;

21 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for
22 purposes of the investigation. The government proposes that the original storage media
on which the Search Warrant Data was placed plus a full image copy of the seized Search
23 Warrant Data be retained by the government.

1 e. If the person from whom any Search Warrant Data was seized requests the return
2 of any information in the Search Warrant Data that is not set forth in Attachment B,
3 Section II, that information will be copied onto appropriate media and returned to the
4 person from whom the information was seized.
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24